Analyse d'impact RGPD : faut-il l'illustrer d'une matrice des risques, et si oui, laquelle ?

Par Bruno RASLE
bruno_rasle@halte-au-spam.com

Paris, le 20 mars 2026

L'analyse d'impact est l'une des grandes avancées du RGPD et un levier puissant pour viser la conformité d'un traitement susceptible de faire peser des risques élevés sur les personnes concernées. C'est aussi l'une des tâches les plus complexes qu'abordent avec précaution - voire appréhension - les responsables de traitement sous la houlette de leur DPO. L'exercice se matérialise par un livrable soumis au responsable afin qu'il l'endosse et prenne des décisions pour faire notamment en sorte que les mesures de traitement des risques soient opérationnelles avant la mise en œuvre du traitement. Même si le RGPD ne l'exige pas, l'habitude a été prise d'illustrer ce document d'une matrice des risques. Est-ce une bonne idée ? Quels sont les objectifs visés par cette insertion ? Comment la concevoir et y positionner les événements redoutés et les risques bruts et résiduels associés ? Y-a-t-il des pièges à éviter, des biais ou des limites à cette approche ? Et quelles sont les caractéristiques d'une « bonne » matrice des risques dans le cadre d'une AIPD formalisée au titre du RGPD ?

Data Protection (or Privacy) Impact Assessment is one of the major advances of the GDPR (along with data breach notification) and a powerful lever for ensuring compliance in processing operations that are likely to pose high risks to data subjects. It is also one of the most complex tasks, which data controllers approach with caution – even apprehension – under the guidance of their DPOs. The impact assessment takes the form of a deliverable that should be submitted to the controller for approval. It has become customary to illustrate this document with a risk matrix. Is this a good idea? What are the objectives of including it? Are there any pitfalls to avoid? And what are the characteristics of a "good" risk matrix in the context of a formalised DPIA under the GDPR?

L'auteur a présenté les présents travaux le vendredi 20 mars 2026 dans le cadre de l'Université AFCDP du DPO 2026.

L'AIPD est sans doute l'un des leviers les plus puissants au service du DPO[1]

Comme je l'ai indiqué dans mon article de septembre 2022 intitulé « Faut-il être parano pour faire un bon PIA ? », l'obligation dans certains cas de réaliser une analyse d'impact sur la protection des données (ou DPIA, pour *Data Protection Impact Assessment*) est à mon sens l'un des plus formidables leviers à la disposition d'un DPO pour mener son organisme sur le chemin de la conformité, sans que cela soit pour autant un exercice facile[2]. Et, au sein de cet exercice, il en est un qui présente ses propres défis, celui de produire une matrice des risques qui propose « *une approche simplifiée du réel, facilement compréhensible par tous* » comme l'indiquent Raphaël De Vittoris et Sophie Cros dans leur ouvrage « *Déjouer les risques* » (Dunod, 2024). Comment obtenir puissance de synthèse et clarté visuelle concernant une abstraction complexe qu'est le risque ? Tel est le sujet du présent papier.

Pourquoi enrichir une AIPD d'une visualisation des risques ?

Dans son article 35, le RGPD ne fait aucune obligation de faire figurer une quelconque représentation des risques dans une AIPD et les lignes directrices concernant l'analyse d'impact relative à la protection des données du G29 (WP 248 rév. 01 modifiées et adoptées en dernier lieu le 4 octobre 2017) n'abordent même

[1] Le DPO « pilote » la réalisation d'une AIPD, il ne lui revient pas de la « faire ».

[2] Cf. « *Cinq versions de PIA/AIPD avant d'arriver à la bonne* », Bruno Rasle, Août 2024. Si l'analyse d'impact est *a priori* un document en priorité à vocation interne, il pourra être demandé par des auditeurs externes (et par la CNIL dans le cadre d'une mission de contrôle), ce qui justifie une grande attention lors de sa rédaction.

pas ce sujet. Notons également que le téléservice publié par l'autorité espagnole ou le modèle mis à disposition par l'ICO ne prévoient pas d'illustration – même si les dernières AIPD publiées par l'autorité britannique en comprennent, comme celle portant sur le traitement associé à CoPilot[3]. J'avoue avoir trouvé laborieuse (pour ne pas dire indigeste) la lecture de l'AIPD réalisée pour le compte du Ministère de la Justice et de la Sécurité néerlandais sur Microsoft 365 : l'analyse comprend plus de 130 pages de texte. Il faut attendre la page 127 pour trouver une unique matrice 3x3 sur laquelle sont positionnés les risques bruts (De façon surprenante, le document ne présente aucune matrice positionnant les risques nets[4]). Il en est de même dans le « *DPIA Microsoft 365 Copilot* » publié fin 2024 par le même ministère et qui comprend 183 pages. La plupart des mesures de traitement des risques identifiés devant être mises en œuvre par Microsoft, est-ce à dire que l'auteur de l'AIPD n'a pas voulu considérer leur mise en œuvre comme acquise ?

Pour inciter mes consœurs et confrères DPO à insérer une illustration qui permet de visualiser les risques et leur niveau au sein d'une analyse d'impact RGPD, je pourrais reprendre un passage de mon article de mars 2020 intitulé « *Collègues DPO : Le bilan annuel est un outil précieux – Faisons-en une bonne pratique* » dans lequel j'abordais la question suivante : « *Mon bilan peut-il être illustré ?* ». Voici l'extrait en question, qui peut s'appliquer sans problème à notre sujet : « *Le document doit être conçu pour être lu et compris par le responsable de traitement. Voici quelques recommandations concernant le fond et la forme d'un rapport destiné à être lu, à être compris et à être mis à profit par une direction, sur une thématique proche de celle de la conformité : celle de la sécurité informatique. Elles sont tirées du livre « La fonction RSSI », écrit par un membre de l'AFCDP, Bernard Foray : « Penser KISS (Keep it Simple & Stupid), Soigner la sémantique, Penser Comparaison (à la fois interne et externe), Penser Durée et Contexte, Penser Visuel-Vendeur-Sexy ».* ».

La représentation graphique des risques est donc avant tout un outil de communication interne, qui sert de support visuel lors des réunions avec les parties prenantes[5], visant à présenter de façon synthétique les événements redoutés et à évaluer leurs conséquences par rapport à leur probabilité de réalisation. Cette matrice est destinée en priorité au responsable de traitement, à qui l'analyse d'impact sera soumise pour signature car elle en facilite la compréhension (en soutien du texte) comme le recommande le NIST[6] dans son document *Guide for conducting Risk Assessment* : *« Tâche 3-1 : Communiquer et partager les résultats de l'évaluation des risques auprès des décideurs de l'organisme afin de soutenir les mesures prises pour y répondre. L'objectif de cette étape est de s'assurer que les décideurs disposent des informations appropriées relatives aux risques nécessaires pour éclairer et orienter leurs décisions en matière de risques. Les organismes peuvent communiquer les résultats de l'évaluation des risques de différentes manières (par exemple, réunions d'information à l'intention des cadres, rapports d'évaluation des risques, tableaux de bord).* ». Je n'ai trouvé que le Commissariat à la protection de la vie privée du Canada, dans son guide au sujet de EFVP (Evaluation des Facteurs relatifs à la Vie Privée) pour recommander, parmi les « pratiques exemplaires », l'utilisation d'outils visuels, comme des tableaux ou des diagrammes.

Selon son type, ses caractéristiques et sa qualité (et dans le cadre d'une analyse d'impact RGPD), l'illustration des risques peut aussi mettre en évidence les points importants, valoriser le travail réalisé (en montrant le passage des risques bruts aux risques nets[7]) et faciliter le suivi du plan d'action, en affectant, par exemple,

---

[3] « *Data Protection Impact Assessment (DPIA) – Microsoft CoPilot 365* », ICO, Draft, 2024

[4] Le ministère de la justice et de la sécurité néerlandais semble avoir évolué à ce sujet car, en décembre 2025, il a publié un cadre qui permet d'évaluer la qualité des AIPD produites au sein des entités rattachées à ce ministère. Concernant les risques pour les personnes concernées, le niveau à atteindre est ainsi décrit : « *Tous les risques sont décrits sur la base de scénarios réalistes. Une matrice des risques dans laquelle les risques sont répertoriés est incluse. Les risques bruts et nets y sont clairement indiqués.* ».

[5] Cf. « *Une communication améliorée : Un registre des risques clair et structuré favorise une meilleure communication et la collaboration entre les parties prenantes, en veillant à ce que tout le monde comprenne le paysage des risques de l'organisation*. » dans le document *NIST SP 800-30 Guide for conducting Risk Assessment* - September 2012

[6] *National Institute of Standards and Technology*

[7] Dans ce document, j'utilise le terme de *risque brut* pour désigner le risque avant tout traitement (plus rarement, on rencontre les sémantiques *inhérent* ou *intrinsèque*) et les termes *risque résiduel* ou *risque net* pour désigner le risque restant une fois mises en place toutes les mesures de maîtrise des risques. Lors de mes formations, pour illustrer la différence entre les deux notions, je pose la question suivante :

un pilote pour chaque risque[8], en vérifiant la bonne mise en œuvre des mesures de traitement, en créant des indicateurs ou en permettant de positionner des revues ou des audits. Elle peut aussi être l'une des seules informations lues par le responsable de traitement, si celui-ci a peu de temps à consacrer à l'exercice (C'est pourquoi il est recommandé de positionner un exemplaire de l'illustration des risques au début du document, dans la synthèse managériale).

Au sein des nombreuses AIPD qu'il m'a été donné de consulter, je n'ai jamais encore observé d'arborescence inspirée par celle proposée par la norme ISO 13849-1:2023 (norme relative à la sécurité des machines), sans que je sois surpris par cette absence. Dans l'exemple (Fig. 1), l'arborescente attribue un niveau issu de la gravité de la blessure (S), de la fréquence et/ou de la durée d'exposition au phénomène dangereux (F) et de la possibilité d'éviter le phénomène dangereux ou d'en limiter les dommages (P).

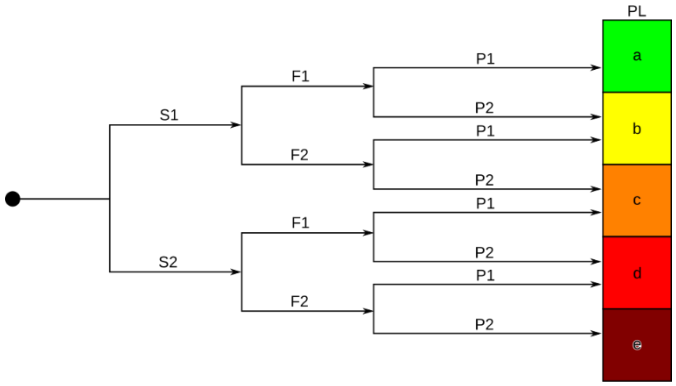


Figure 1 : Arborescence ISO 13849-1

Je regrette également la sous-utilisation du diagramme d'Ishikawa (ou diagramme des causes et effets), en arêtes de poisson, qui accompagne une approche systématique pour analyser un problème dont les causes possibles sont multiples : on part du résultat (du problème) - c'est à dire la tête du poisson-, et les arêtes sont les causes ou les facteurs potentiels. Il s'avère très utile lors des discussions autour des mesures à appliquer pour traiter un risque (Exemple : lors d'un incendie, les pompiers commencent par couper l'arrivée de gaz).

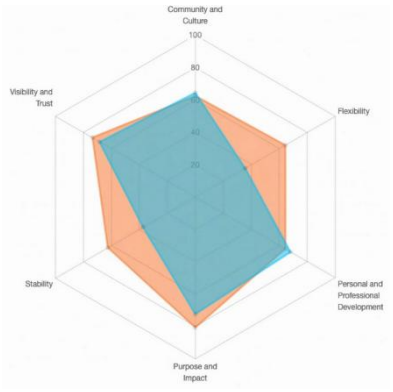


Figure 2 : Exemple de Radar Chart (ou Spider Chart)

En revanche, j'aurais pu m'attendre à rencontrer des illustrations en toile d'araignée (ou *Radar Chart,* Cf. Fig.2) dans laquelle chaque axe correspond à un risque. Plus le niveau de celui-ci est jugé élevé, plus le point est éloigné du centre. Les points sont ensuite reliés entre eux pour constituer une surface. Moins cette surface est grande, moindre est l'exposition aux risques.

Cette illustration permet de représenter simultanément les risques bruts et les risques nets (on visualise d'un seul coup d'œil l'effet des mesures de réduction des risques) et autorise l'ajout d'une ligne d'acceptabilité, mais elle ne permet pas de prendre connaissance des évaluations en vraisemblance et gravité qui ont été attribuées à chaque événement redouté, ces informations étant renvoyées dans le texte.

« *Si on vous en donnait le choix, quelle somme préféreriez-vous voir verser sur votre compte en banque à la fin de chaque mois ? Votre salaire brut (avant toute retenue) ou votre salaire net ?* ».

[8] L'intégration des « propriétaires du risque » parmi les parties prenantes se retrouve également dans la méthode Ebios RM et dans l'ISO 27005.

Dans cette famille d'illustrations, on rencontre peu fréquemment une variante issue de la méthode EBIOS Risk Manager (Fig.3). Elle a notamment été présentée par Philippe Bost, DPO de Clermont-Auvergne-Métropole lors d'un partage d'expérience au sein de l'AFCDP en 2022. L'échelle est ici inversée par rapport à la figure 2 : les parties prenantes les plus exposées aux risques sont celles situées près du centre. Dans cette représentation, la limite verte correspond à la zone de veille (de surveillance), la limite jaune à la zone de contrôle et la rouge à la zone de danger.

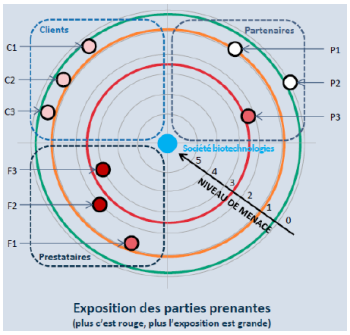


Figure 3 : Autre exemple d'utilisation du Radar Chart

Enfin notons la présence, dans l'outil PIA de la CNIL, d'un diagramme de Sankey[9] simplifié, intégré pour relier visuellement les impacts potentiels, menaces, sources et mesures aux trois types de pertes possibles[10] (confidentialité, intégrité, disponibilité).

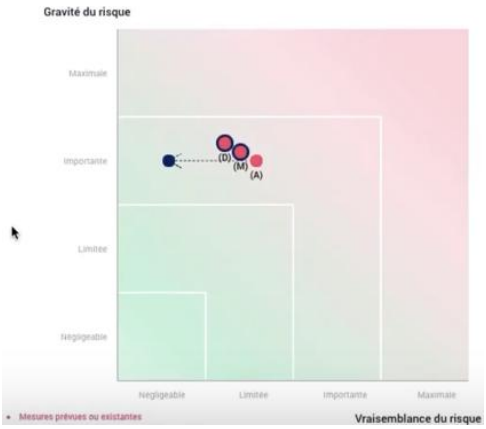


Figure 4 : Extrait de la vidéo de présentation de l'outil PIA de la CNIL (les risques bruts sont en rouge, les nets/résiduels en bleu)

Mais c'est une visualisation en matrice (appelée également *Risk Heat Map* dans la littérature anglo-saxonne) qui semble s'être imposée au sein de la communauté des DPO. Cette habitude provient en fait du monde de l'analyse de risques (et non d'impact), ce qui explique que la CNIL en fasse apparaitre une dans plusieurs de ses documents[11] (comme celui intitulé « *Analyse d'impact relative à la protection des données - Les modèles* », en page 24) et dans son outil PIA. La matrice générée par ce dernier outil présente un axe « vraisemblance du risque » en abscisse un l'axe « gravité du risque » en ordonnée. Ces axes sont ordinaux et comporte chacun quatre niveaux, avec utilisation d'une sémantique unique. Seules deux couleurs sont utilisées, le vert et le rouge, avec utilisation d'un fondu.

Quelle est l'origine de la matrice ?

La matrice a pour origine historique le diagramme de Farmer (Fig.5), certes après adaptation. Frank Reginald Farmer (1914 - 2001) travaillait pour la Direction de la sûreté et de la fiabilité de l'Autorité de l'énergie atomique du Royaume-Uni. En 1967, il a proposé une représentation pour visualiser les risques engendrés pour la société par une technologie, un projet ou une activité (en l'occurrence il s'agissait de sélectionner l'emplacement des centrales nucléaires en tenant compte du risque de fuites d'iode 131[12]). Elle est également appelée « diagramme F-N » dans lequel l'échelle verticale (F) indique la fréquence des événements redoutés, tandis que l'échelle horizontale représente les conséquences (généralement le nombre de décès, N). Sur la partie gauche de la courbe figurent les événements fréquents mais qui ne touchent que peu de personnes, tandis que la partie droite représente les rares incidents faisant des victimes en grand nombre.

[9] Nommé en hommage au capitaine irlandais Matthew Henry Phineas Riall Sankey (1853-1926), qui a utilisé ce type de diagramme dès 1898 dans une publication sur l'efficacité énergétique d'une machine à vapeur, bien que le Français Charles Joseph Minard utilisât ce type de représentation graphique dès 1869.

[10] Personnellement, je n'ai jamais intégré un tel schéma, n'ayant pas saisi son apport.

[11] L'expert qui, au sein de la CNIL (après avoir œuvré au sein de l'ANSSI), a posé les bases de la doctrine de la Commission en matière d'analyse d'impact s'est appuyé sur l'ISO27001 (Il a également été Président du club EBIOS).

[12] Voir l'article « *Farmer's diagram, or F-N curve - Representing society's degree of catastrophe aversion* », par Eric Marsden, juillet 2022

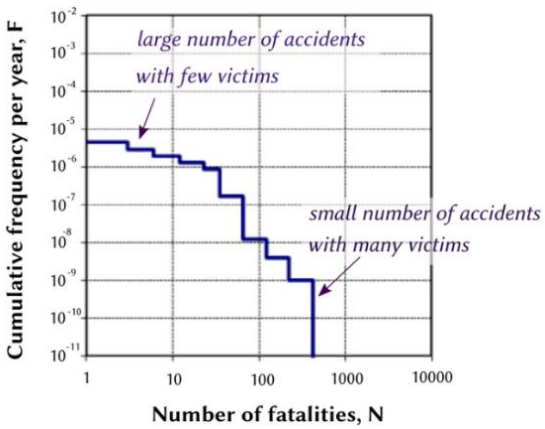


Figure 5 : Diagramme de Farmer

Ce type de représentation est souvent enrichi de limites d'acceptabilité : une ligne supérieure matérialise au-dessus d'elle une zone « intolérable » tandis qu'une ligne inférieure délimite en dessous d'elle une zone où les risques sont considérés comme négligeables. L'espace entre ces deux lignes correspond aux risques qui sont assumés, avec traitement et surveillance. Nous verrons plus loin combien cette notion de « seuil d'acceptabilité » fait sens dans le contexte d'une analyse d'impact au sens du RGPD (pourtant, peu de matrices figurant au sein des AIPD en contiennent).

Il faut commencer par prendre connaissance de l'existant

Avant de s'attaquer à sa première AIPD, la priorité est de prendre connaissance des us et coutumes de l'organisme concernant la gestion des risques et notamment de s'enquérir des représentations qui sont déjà utilisées pour les représenter dans d'autres champs (comme l'appréciation des risques clients, financiers ou opérationnels) ainsi que des échelles qui servent à les qualifier en vraisemblance et en gravité. Si ces approches conviennent à la façon d'appréhender les analyses d'impact au sens du RGPD, il peut être délicat – voire improductif – de s'en écarter, la direction ayant pris l'habitude des représentations qui lui sont présentées de longue date et souhaitant probablement une certaine homogénéité des styles d'illustration (et des échelles) pour permettre quelques comparaisons.

À l'inverse, si vous êtes désigné DPO au sein d'une structure qui a peu d'expérience dans la gestion du risque, c'est peut-être vous qui allez donner le « la » en implantant votre méthode qui pourrait être par la suite reprise pour illustrer d'autres types de risques qui pèsent sur l'organisation.

La matrice n'est pas « isolée »

La matrice des risques n'est que le rendu visuel de la méthode utilisée pour évaluer chaque événement redouté. Elle est donc en lien étroit avec l'approche retenue[13]. Même si cela n'est pas le sujet du présent article, il ne m'est donc pas possible de traiter correctement du rendu visuel (la matrice) sans aborder *a minima* le cheminement qui nous permet d'y parvenir (de plus, la personne qui a piloté l'analyse d'impact RGPD doit être en mesure de répondre à l'une des questions légitimes que peut soulever un dirigeant à qui l'on demande d'endosser les risques résiduels : « *Mais comment diable avez-vous positionné ce risque à cet endroit dans la matrice ?* »). Aussi, même s'il ne s'agit pas du sujet que je traite dans le présent document, je suis amené à en proposer une synthèse.

[13] Actuellement, le RGPD n'impose aucune méthode, du moment que les critères d'éligibilité listés dans les lignes directrices sont respectés. La méthode retenue devrait être documentée, « défendable », reproductible et vérifiable et produire un livrable compréhensible. À vous de choisir la méthode qui vous semble la plus appropriée (Celle promue par la CNIL n'est pas obligatoire et ne donne en aucune façon l'assurance de produire une AIPD sur laquelle la Commission n'aura aucun reproche à formuler), en prêtant attention au fait que la quasi-totalité des méthodes existantes ont été pensées à l'origine « risques pour l'organisme » et non pas pour les personnes concernées.

On distingue deux grandes familles de méthodes[14] : celles basées sur le calcul (dites « quantitatives) et celles basées sur l'humain (dites « qualitatives »). La première famille se veut objective (neutre), comme celle décrite dans le papier intitulé *Quantitative Privacy Risk Analysis*, publié en 2021 par R. Jason Cronk et Stuart S. Shapiro. La vraisemblance y est déterminée par un calcul qui tient compte de quatre facteurs : l'opportunité, la motivation, la capacité à faire et la difficulté à faire. L'opportunité est exprimée par le nombre de fois (dans une période de temps donnée) où le facteur de risque est présent. La motivation est une variable aléatoire qui représente la probabilité qu'un acteur de la menace saisisse une opportunité. La capacité est une variable aléatoire qui représente le niveau de compétences et des ressources qui doivent être mobilisés pour mener à bien une tentative. La difficulté est une variable aléatoire qui matérialise le niveau des obstacles qui s'opposent à la réalisation d'une tentative. Le calcul se fait en trois étapes : Il faut d'abord calculer la fréquence des tentatives qui est fonction de l'opportunité et de la motivation et est calculée par la méthode de Monte Carlo[15], puis, à nouveau, grâce à une simulation de type Monte Carlo, la vulnérabilité est calculée à partir de la capacité et la difficulté (à faire), et enfin la fréquence est dérivée de la fréquence des tentatives et de la vulnérabilité (à nouveau, grâce à une simulation de type Monte Carlo).

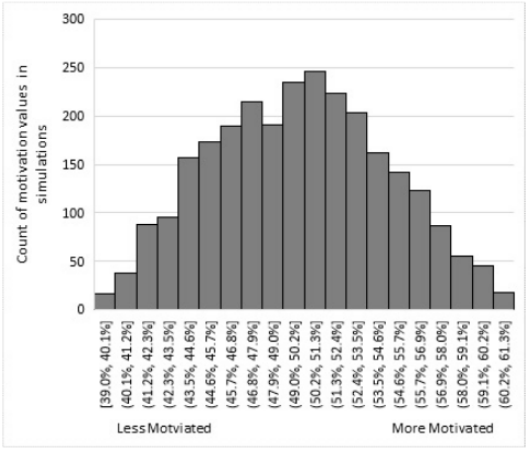


Figure 6 : Histogramme des résultats de simulation pour différents pourcentages de motivation possibles

Malheureusement, le document ne fournit aucun exemple concret et aisément compréhensible d'application de cette méthode. Cette approche nécessite de disposer d'une sinistralité[16], ce qui est relativement rare. Dans ce cas, la matrice associée est dotée d'échelles quantitatives (et non pas ordinales[17]). Dans le cadre des Lundi de la cyber, j'ai suivi avec intérêt une présentation par la société Citalid de la méthode qu'elle a développée pour évaluer a priori le coût d'un sinistre et décider s'il faut investir pour le contrer. Constatant que les données sur le risque cyber manquent cruellement, ils ont créé un modèle bayésien (utilisant des simulations de Monte-Carlo) qu'ils ont calibré avec les quelques données initialement à disposition et qu'ils mettent à jour dès que de nouvelles données sont disponibles. Ainsi, les résultats sont sensés s'améliorer à mesure que les données de sinistralité affluent. Le modèle tient compte de la fréquence de la menace, de la probabilité de sinistre, de la probabilité de subir des pertes et de l'ampleur de ces dernières. Cette méthode, pensée « risques cybersécurité » n'est pas applicable telle quelle aux AIPD dans le cadre du RGPD. De plus, comme me l'ont confié leurs auteurs, elle se concentre sur les « adversaires frontaux » et ne prend pas en compte les sources de risques internes (mauvaise conception, mauvaise qualité logicielle, erreur humaine, non-respect des consignes, etc.).

La seconde famille (la « qualitative ») est plus subjective et s'appuie essentiellement sur le ressenti des parties prenantes à l'analyse d'impact (le chef de projet MOA, le chef de projet MOE, les RSSI, le Risk Manager, le

[14] Dans son document *Compendium of risk-managements frameworks with potential interoperability*, L'ENISA décrit une vingtaine de méthodes d'analyse de risques.

[15] La simulation de Monte-Carlo, est une méthode algorithmique visant à calculer une valeur numérique approchée en utilisant des procédés aléatoires, c'est-à-dire des techniques probabilistes.

[16] Dans son document *Risikoanalyse und Datenschutz- Folgenabschätzung*, le délégué bavarois à la protection des données donne la priorité aux méthodes qualitatives et se montre prudent quant à l'utilisation des éléments de sinistralité : « *La probabilité d'occurrence peut donc être étayée par les circonstances existantes, par sa propre expérience et celle d'autres personnes, ainsi que par des statistiques. En ce qui concerne les statistiques, il convient toutefois de tenir compte des conditions dans lesquelles elles ont été établies, car elles ont été conçues pour un usage spécifique et ne peuvent donc pas être transposées telles quelles aux besoins particuliers de l'institution. En outre, l'interprétation des résultats statistiques est en principe source d'incertitudes.* »

[17] « *En mathématiques, on appelle nombre ordinal un objet permettant de caractériser le type d'ordre d'un ensemble bien ordonné quelconque, tout comme en linguistique, les mots premier, deuxième, troisième, quatrième, etc. s'appellent des adjectifs numéraux ordinaux, et servent à préciser le rang d'un objet dans une collection, ou l'ordre d'un événement dans une succession.* » - Source Wikipedia

responsable PRA/PCA, le sous-traitant, le représentant des personnes concernées… et bien sûr le DPO). Forts de leur expérience, plus ou moins conscients des incidents déjà survenus et influencés par leur *a priori*, ces acteurs attribuent des notes de vraisemblance et de gravité à chaque événement redouté. L'actuelle méthode de la CNIL est représentative de cette approche, qui propose des échelles ordinales comprenant chacune quatre valeurs (en l'occurrence, se sont le rédacteur et l'évaluateur qui s'expriment à ce sujet).

Sans surprise, chaque formule a ses avantages et ses inconvénients[18] et c'est pourquoi les méthodes les plus utilisées actuellement sont « semi-qualitatives », en ce sens qu'elles tentent d'encadrer les évaluations subjectives dans un cadre rassurant ayant un aspect « scientifique ». La méthode de l'ENISA pour évaluer la gravité d'une violation de données en est un bon exemple, avec une superbe équation qui inspire confiance : SE = DPC x EI + CB, équation dans laquelle DPC (*Data Processing Context*) résulte d'un calcul qui dépend principalement du type de données violées, de leur classification, du volume de données et de leur fraicheur, EI (*Ease of Identification*) correspond à un niveau parmi quatre relatifs à la « facilité » avec laquelle un individu pourrait être identifié à partir des données violées[19] et CB (*Circumstances of the Breach*) pour tenir compte du contexte spécifique[20]. Cette formule produit un résultat que l'on positionne alors sur une échelle ordinale de quatre niveaux (*Low*, *Medium*, *High* et *Very High*). Appliquée à la violation de données personnelles des clients de Deezer qui a valu à son sous-traitant israélien *Mobius Solutions Ltd* une sanction d'un million d'euros de la part de la CNIL[21], cette formule donne un résultat de 3, c'est à dire *High*. Si Deezer avait pris la précaution de confier à son prestataire uniquement des données pseudonymisées (qui étaient suffisantes pour réaliser la prestation demandée), le résultat n'aurait été que de 1,5, c'est à dire *Low*. C'est une façon d'objectiver auprès de la direction la nécessité de mettre en œuvre certaines mesures de traitement des risques. Malgré tout, on perçoit bien que, selon les valeurs sélectionnées pour réaliser les calculs (les moyennes ? les médianes ? les extrêmes ?), le résultat final peut varier considérablement (ce que j'ai expérimenté sur plusieurs cas réels), ce qui rend le caractère de rigueur algorithmique discutable. Dans son document « *Recommendations for a methodology of the assessment of severity of personal data breaches* », l'ENISA invite d'ailleurs à ne pas accorder une confiance aveugle à l'apparence« scientifique » de cette approche : « *Il convient de rappeler que tant les responsables du traitement des données que les autorités compétentes doivent faire preuve d'une vigilance particulière lorsqu'ils traitent des cas qui, en raison de leurs spécificités, ne peuvent être correctement évalués à l'aide de cette méthodologie.* ».

Voici un autre exemple de méthode semi-qualitative, celle suggérée par la CNIL en 2012 (cette approche a depuis été abandonnée) : Elle consistait à commencer par considérer la vulnérabilité des supports (de 1. « *Négligeable - Il ne semble pas possible de réaliser la menace* » à 4. « *Maximal – Il est extrêmement facile de réaliser la menace* »), puis à estimer la capacité des sources de menace pour réaliser leur méfait (de 1. « *Négligeable - Elles ne semblent pas avoir de capacité* » à 4. « *Maximal - Elles ont des capacités illimitées* »). Il fallait ensuite additionner les deux résultats obtenus. Si le total obtenu est inférieur à 5, alors la vraisemblance est négligeable (1), s'il est égal à 5, la vraisemblance est limitée (2), s'il est égal à 6, la vraisemblance est importante (3) et si le total est supérieur à 6, alors la vraisemblance est maximale (4). La CNIL précisait que « *Cette cotation peut être augmentée ou diminuée par d'autres facteurs, comme l'ouverture sur Internet ou une grande hétérogénéité du système* ».

---

[18] Il n'existe pas à ma connaissance de méthodes idéales, exemptes de tout défaut, pour évaluer les risques. L'important est qu'elles soient utilisées avec une bonne compréhension de leurs biais et limites.

[19] Cela soulève une question à laquelle je n'ai pas (encore) trouvé de réponse satisfaisante : Compte tenu du gisement énorme de données personnelles qui ont fait l'objet de violations de données (nom, prénom, date et lieu de naissance, numéro de sécurité sociale, adresse email, etc.) et qui ont été publiées sur le Darknet, ne peut-on considérer que ces informations sont « publiques » [ce concept n'est jamais défini précisément], ce qui minorerait le facteur EI et le niveau de risque final ?

[20] De façon surprenante, dans son document *PDB Assessment Methodology*, l'ICO utilise une autre version de la même équation, dans laquelle les facteurs DPC et EI sont additionnés (au lieu d'être multipliés) : SE = DPC + EI + CB. L'autorité britannique indique que la méthode n'est pas prescriptive « *et a été adaptée à partir des recommandations de l'ENISA concernant une méthodologie d'évaluation de la gravité des violations de données à caractère personnel* » mais sans donner d'explication sur la raison de cette variante.

[21] Cf. Délibération SAN-2025-014 du 11 décembre 2025

The complete steps for computing likelihood are as follows:

1. Find the value of *exploitability* for each leaf node in the harm tree.
2. For each exploitation, choose the values of the relevant attributes of the risk source most likely to exploit the privacy weakness leading to the harm.
3. Find out the likelihood of each of these exploitations from the above *exploitability* value and values of the relevant risk source attributes.
4. Compute the likelihood of each feared event and harm according to the following rules[30], where P_i is the likelihood of ith child node:

   R1. AND node with independent child nodes: $\prod_i P_i$.

   R2. AND node with dependent child nodes[31]: $Min_i(P_i)$, i.e., minimum of the likelihoods of the child nodes.

   R3. OR node with independent child nodes: $1 - \prod_i (1 - P_i)$.

   R4. OR node with dependent child nodes[32]: $\sum_i P_i$.

Figure 7 : Méthode PRIAM pour évaluer la vraisemblance

La méthode PRIAM[22] (*Privacy Risk Analysis Methodology*) utilise les deux approches, mais de façon successive. Pour ses auteurs, cette approche combinée permet d'éviter les biais de chaque approche : « *Les probabilités peuvent être calculées de différentes manières, soit symboliquement (sur la base d'une échelle fixe de niveaux tels que « négligeable », « limité », « significatif », etc.), soit à l'aide de valeurs numériques (probabilités). Chaque approche présente des avantages et des inconvénients. En règle générale, les probabilités peuvent être difficiles à estimer pour les valeurs d'entrée et peuvent sembler difficiles à appréhender par les décideurs. À l'inverse, les valeurs symboliques sont parfois trop floues et peuvent conduire à des interprétations différentes* ».

Pour établir la vraisemblance d'un risque, la méthode PRIAM commence par établir des « arbres des dommages[23] », commence par traiter des valeurs d'entrée symboliques, les convertit en valeurs numériques pour pouvoir les associer aux arbres de dommages, puis les transcrit à nouveau en valeurs symboliques pour la sortie finale. Je n'ai pas eu connaissance d'AIPD qui ait été réalisée selon cette méthode.

La méthode qualitative la plus connue est l'EBIOS Risk Manager, dans laquelle les risques sont recensés et évaluées lors d'ateliers[24] auxquels participent les parties prenantes. Rédouane Djedir, DPO de la Bred (groupe Banque Populaire), lors de son intervention intitulée « *Au secours j'ai trop de PIA à réaliser !* » dans le cadre de l'Université 2025 des DPO de l'AFCDP, a précisé qu'il participe à l'atelier au cours duquel sont recensés et évalués (en vraisemblance et gravité) les risques aux côtés des représentants de la direction Métier concernée, de la DSI, du RSSI et éventuellement des sous-traitants. En revanche, il se tient volontairement éloigné de l'atelier au cours duquel les parties prenantes identifient les mesures de traitement les plus pertinentes, pour responsabiliser ces acteurs.

Cette méthode a beaucoup d'avantages, car elle est basée sur une analyse humaine. Mais elle génère une certaine charge[25] (mobilisation importante de nombreuses personnes) et surtout peut souffrir d'un phénomène d'auto-censure (personne n'ose parler ou évoquer des incidents passés, dont certains n'ont pas été portés à la connaissance du DPO), voire produire des consensus obtenus de façon biaisée du fait du conformisme social sur les décisions d'un individu au sein d'un groupe, comme l'a mis en lumière le psychologue Solomon Asch, de l'Université de Pennsylvanie, en 1951 (Dans l'expérience qu'il a pilotée, un sujet « naïf » fini par déclarer qu'une ligne, manifestement plus courte que les autres, ne l'est pas, rejoignant ainsi l'avis des autres membres du groupe, des complices ayant eu pour consigne de tous formuler une

[22] Sourya Joyee De, Daniel Le Métayer. *PRIAM: A Privacy Risk Analysis Methodology*. [Research Report] RR-8876, Inria - Research Centre Grenoble – Rhône-Alpes. 2016.

[23] La racine d'un arbre désigne un dommage. Les feuilles représentent les faiblesses en matière de confidentialité exploitées par la source de risque la plus probable pour le dommage en question et sont représentés par des paires (faiblesse en matière de confidentialité, source de risque). L'arbre est structuré en branches menant au dommage.

[24] La méthode par ateliers appartient à la famille des analyses SWIFT (pour « *Structured What-If Technique* », ou technique structurée de simulation de scénarios).

[25] Estimée à 7h30 par participant, sans compter le temps nécessaire à l'organisation des ateliers, soit environ entre 180 et 200 heures/homme au total.

mauvaise réponse.). Pour ma part, j'ai adapté la méthode de Delphes[26] (que j'enseigne dans le cadre de ma formation « *Réaliser une Analyse d'Impact - De la théorie à la pratique* ») qui permet d'échapper à ce piège et de moins peser sur les parties prenantes. En cas d'utilisation de cette approche, il appartient au DPO de contrer les biais[27], comme celui de la récence qui aboutit à surévaluer des risques qui se sont produits récemment (et, inversement, de sous évaluer les plus anciens).

Mais au final, c'est bien l'avis du responsable de traitement (qui, selon le RGPD, « effectue » l'AIPD) sur les risques et leur gravité qui est prépondérant. S'agissant de risques qui pèsent sur autrui, certains ne poussent pas très loin leur raisonnement. Je pense par exemple au témoignage du dirigeant de Voyageurs du Monde, après s'être fait exfiltrer 10.000 passeports[28] : « *Ils font les malins pour pas grand-chose…/… Il ne s'agit que de copies et aucune donnée biométrique n'a été recueillie par les pirates …/… Franchement, on n'est pas inquiets* », ou plus récemment les déclarations d'un président d'une fédération départementale de chasseurs du Jura après la mise en vente par un pirate informatique sur le *Darkweb* des données de 1.416.000 chasseurs[29] : « *Je ne suis pas inquiet. Je ne vois pas ce qu'on peut faire de ces informations. Ce n'est pas vital.* ». Quand on sait que, à la suite du vol des données des membres de la fédération de tir, la cyberattaque avait été suivie d'agressions et de vols d'armes à feu auprès de plusieurs adhérents dans plusieurs villes de France[30]…

Être conscient de la « tare » originelle

La plupart des méthodes créées ces dernières années pour réaliser une analyse d'impact au sens du RGPD sont en fait des adaptations de processus pensés à l'origine pour mener des analyses de risques. Il faut donc avoir en tête certaines différences essentielles entre les deux approches pour mieux comprendre la piètre qualité de la plupart des AIPD réalisées en suivant ces méthodes et surtout prendre des mesures pour traiter les biais.

Pour commencer, là où une analyse d'impact s'intéresse au sort des personnes concernées[31], l'analyse de risques se focalise sur ceux qui pèsent sur l'organisme[32]. En quelque sorte, une AIPD est un exercice altruiste, alors que l'analyse de risques est une démarche égoïste. En réalisant une analyse de risques, l'organisme décide de sa « prise de risque », pour lui-même. Le risque est alors la coexistence d'un aléa (les conséquences potentielles des actions entreprises) et d'un enjeu. Lorsque l'organisme prend un risque pour lui-même, il entreprend une action avec un espoir de gain et/ou une possibilité de perte. Mais en réalisant une AIPD, l'organisme décide du niveau de risque… qu'il va faire courir à des tiers. Le responsable de

---

[26] La méthode Delphi a été conçue dans les années 1950 par Olaf Helmer et Norman Dalkey, de la *Rand Corporation*. Son nom fait référence à l'Oracle de Delphes, une prêtresse du temple d'Apollon dans la Grèce antique, célèbre pour ses prophéties.

[27] Les biais cognitifs peuvent altérer le jugement, influencer les décisions et amplifier les risques d'erreur, comme le biais de confirmation ou celui d'ancrage. Le biais de groupe survient lorsqu'un groupe prend des décisions pour maintenir la cohésion et éviter les conflits, même si cela signifie ignorer des options pertinentes ou adopter des solutions moins optimales. Le biais de récence consiste à accorder plus d'importance aux informations les plus récentes. Dans une étude d'impact, cela peut mener à surévaluer des événements récents au détriment d'une vision d'ensemble, ce qui peut conduire à des décisions inappropriées.

[28] Cf. « *Mon analyse de la cyberattaque qui a touché Voyageurs du Monde* », Bruno Rasle, 8 juin 2023

[29] Cf. « *Des hackers s'emparent des données personnelles : plus d'un million de chasseurs pourraient être concernés* », par Emmanuel Deshayes, France 3 Bourgogne Franche-Comté, 22 janvier 2026

[30] Là aussi, l'application de la formule de l'ENISA pour évaluer la gravité pour les personnes concernées peut aboutir sur des résultats très différents suivant les valeurs d'entrée sélectionnées.

[31] Et on ne répétera jamais assez que les risques qui doivent être pris en compte sont tous ceux qui pourraient impacter les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel. Les lignes directrices WP248 insistent sur ce point : « *La référence aux droits et libertés des personnes concernées vise principalement les droits à la protection des données et à la vie privée, mais s'entend également, le cas échéant, pour d'autres droits fondamentaux, tels que la liberté de parole, la liberté de pensée, la liberté de circulation, l'interdiction de toute discrimination, le droit à la liberté ainsi que la liberté de conscience et de religion.* ». Aussi, je suis surpris d'entendre que les RFIA qui seront réalisées dans le cadre du RIA prendront *enfin* en compte l'ensemble des droits et libertés. N'est-ce pas le signe que les AIPD sont souvent réalisées petits bras ?

[32] L'impact d'un événement redouté sur les clients n'est considéré que par le prisme de l'impact sur l'entreprise (perte de parts de marché, baisse du panier moyen, etc.).

traitement est intéressé par l'enjeu (ce qu'il a à gagner) mais ne supporte pas l'aléa, qu'il fait peser sur les personnes concernées, la plupart du temps sans même les en informer[33] ni les consulter. Certes, l'article 35.9 du RGPD dispose que « *Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu* », mais il est rare que cela soit réalisé. Pourtant, qui mieux que les personnes concernées - les éventuelles futures victimes - sont les mieux placées notamment pour évaluer l'impact que les événements redoutés pourraient avoir sur eux[34] ? Aurait-on peur de leur réaction à leur lecture de la matrice des risques réalisée ?

Deuxièmement, les méthodes d'analyse de risques se focalisent sur les risques sécuritaires, les plus souvent techniques, et sur les attaques[35]. Ainsi, dans le rapport « *Analyse d'impact relative à la Protection des Données : le cas des voitures connectés* » publié en 2021 par la chaire « Valeurs et Politiques des Informations Personnelles » de l'Institut Mines-Télécom[36], je relève le passage suivant : « [La méthode de la CNIL] *est néanmoins critiquable sur plusieurs points .../... en se focalisant uniquement sur la conformité informatique.../... l'analyse des risques pour la protection des données personnelles par le biais des risques à la sécurité informatique dénature la première catégorie d'analyse* ». Cela ressort nettement, par exemple, dans le document « *EBIOS Risk Manager - Une autre méthode d'évaluation de la vraisemblance* », dans lequel tous les critères sont axés autour des notions d'attaques et d'attaquants[37] (par exemple, celui intitulé *Sentiment d'impunité*, qui définit la peur de l'attaquant de se faire prendre en flagrant délit). Et dans le livret dédié à la même méthode publié par l'ANSSI, aucun des exemples qui listent les sources de risques n'évoque les collaborateurs, les concepteurs d'application, les développeurs ou les incidents matériels… alors que de nombreuses situations préjudiciables pour les personnes concernées ont pour origine un non-respect des consignes ou une mauvaise qualité logicielle, autant de risques qui sont trop souvent oubliés. L'organisme ayant échoué à lister ce type d'événement redouté, l'AIPD sera de mauvaise qualité puisqu'aucune mesure de traitement des risques ne sera mise en place. Je me rappelle un cas où, à cause de l'un de nos traitements, une personne concernée s'est retrouvée interdite bancaire. L'origine du risque n'étant pas sécuritaire, ce risque n'avait pas été identifié et était resté non traité. Dans une telle situation, il revient au DPO de se rapprocher de la personne chargée de rédiger le cahier de recette afin de détecter les défauts de conception. Dans un autre cas, l'événement redouté avait pour source une information insuffisante des personnes (la mesure a donc été de renforcer celle-ci). Là encore, les méthodes dérivées de l'analyse de risque passent trop souvent à côté de ce genre de choses. Il est donc crucial que les DPO « n'abandonnent » pas la réalisation des AIPD aux seuls RSSI et informaticiens et veillent à étendre la réflexion bien au-delà des risques sécuritaires et techniques (il convient par exemple de veiller à l'absence de détournement de finalité).

Troisièmement, les méthodes d'analyse de risque ne considèrent souvent que trois types d'incident : les pertes de confidentialité, les pertes d'intégrité et les pertes de disponibilité. S'il faut effectivement en commencer par-là, il faut pousser la réflexion plus loin car il existe des événements redoutés qui n'appartiennent à aucune de ces familles[38]. J'ai souvenir d'un projet dans lequel les personnes concernées

---

[33] La prise de risque est qualifiée alors d'involontaire.

[34] Dans son « *Traité de riscologie* » (Imestra Editions, 2009), Georges Jousse évoque le facteur de sentimentalité qui fait que la valeur de la conséquence d'un événement redouté n'est pas la même selon que la personne qui l'évalue se sent concernée ou non par le risque.

[35] « *L'objectif principal de la gestion des risques est de protéger les systèmes d'information (logiciel, matériel, systèmes, composants, services) et les actifs commerciaux, et de minimiser les coûts en cas de défaillance* », ENISA, *Risk Management Standards - Analysis of standardisation requirements in support of cybersecurity Policy*, March 2022

[36] Ce document comporte une comparaison très intéressante entre quatre méthodologies (celle de la CNIL, PRIAM, celle du BSI et celle du NIST) et préconise d'étudier en complémentarité la méthode LINDDUN (pour « *Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance* ») proposée par des chercheurs de l'université belge, Katholieke Universiteit Leuven. Cette méthode permet d'identifier les menaces lors du développement de projets IT.

[37] La méthode se concentre sur « *les menaces intentionnelles et ciblées* ». Et, selon le Club EBIOS, « *l'objectif n'est pas d'identifier tous les risques mais uniquement les plus significatifs* ».

[38] C'est ce qu'indique l'EDPS dans son document *Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation*, July 2019 : « *Bien qu'il existe un lien étroit avec la gestion des risques liés à la sécurité de l'information (car il n'est pas possible*

auraient été dans l'impossibilité de demander à bénéficier d'une prestation sociale alors qu'aucune des trois pertes évoquées *supra* n'auraient été observées. Autre exemple, le risque que le traitement génère un *chilling effect* (effet dissuasif) - le fait que les personnes concernées se sentent empêchées d'exercer un droit, aient tendance à s'autocensurer ou à s'abstenir de mener une activité, par crainte des répercussions (pressions, représailles, préjudices) qu'elles pourraient subir.

Enfin, l'entité qui est au centre de l'attention d'une analyse de risques étant unique (l'organisme qui la mène), on obtient rapidement une liste d'événements redoutés dont les conséquences sont assez faciles à évaluer. Dans ce cas, une matrice des risques unique suffit. À l'inverse, dans le cadre d'une analyse d'impact RGPD, le même traitement peut concerner des personnes physiques qui auront des expositions aux risques très diverses. En cas de survenance de chaque événement redouté, certains ne souffriront d'aucun inconvénient là où d'autres auront à subir des conséquences catastrophiques. Produire alors une seule matrice des risques fait-il sens ? Ne faudrait-il pas plutôt produire une matrice de risque par population homogène[39] et aller jusqu'à étudier des mesures de traitement des risques spécifiques à chaque population ? Certaines méthodes d'évaluation des risques font intervenir la notion d'*Unité d'utilité* qui sert d'unité de valeur pour tenter de juger des impacts pour chaque personne concernée. Ainsi, à la suite d'un accident d'autocar dans lequel plusieurs voyageurs s'en sont sortis avec un doigt coupé, ce même événement sera estimé à un faible nombre unités d'utilité pour un footballeur… et à un nombre bien plus grand pour un violoniste. Comme l'indique Georges Jousse dans son « *Traité de riscologie* », rares sont les cas où la nature de la conséquence est unique pour l'ensemble des victimes. Dès lors, on peut très bien imaginer de produire une AIPD comportant plusieurs matrices, chacune dédiée à une population homogène. Logiquement, les mesures de traitement seraient différenciées (plutôt que globales), pour apporter une protection supérieure aux personnes concernées pour lesquelles l'impact sera le plus élevé. Ainsi, il n'est pas rare que la consultation des dossiers des « clients VIP » (politique, célébrité, etc.) fasse l'objet d'un contrôle renforcé. On pense aussi aux entités autorisées à traiter des données révélant, à leur seule lecture, la qualité de militaire de certaines personnes concernées.

À quoi ressemblent les matrices le plus fréquemment observées en France ?

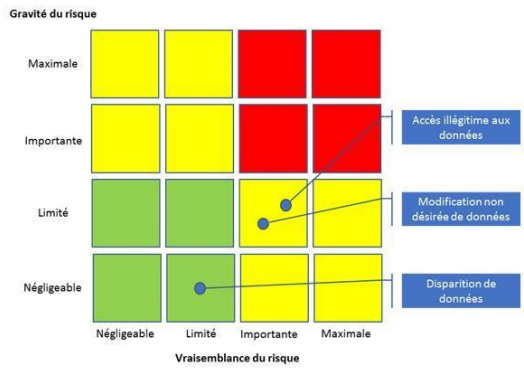


Figure 8 : Matrice des risques fréquemment observée au sein des AIPD (France)

Sans doute du fait de l'outil PIA de la CNIL (et de la reprise dans de nombreux outils du marché destinés à aider les organismes à respecter le RGPD), une norme de fait semble s'être imposée au sein de la communauté des DPO français : une matrice de 4 x 4, avec l'axe « *vraisemblance du risque* » en abscisse et l'axe « *gravité du risque* » en ordonnée. Chez les DPO qui ne génèrent plus la matrice avec l'outil de la CNIL, les couleurs le plus fréquemment observées sont le vert, le jaune et le rouge avec la répartition de la figure 8.

d'assurer une bonne protection des données sans une bonne sécurité des données), les risques à prendre en compte dans le cadre d'une AIPD vont au-delà de ceux qui affectent les objectifs classiques d'une analyse de risque informatique, à savoir la confidentialité, l'intégrité et la disponibilité. ».

[39] C'est ce que semble recommander le Commissariat à la protection de la vie privée du Canada dans son guide relatif au processus d'évaluation des facteurs relatifs à la vie privée : « *Vous devriez envisager l'incidence que pourrait avoir votre initiative sur le droit à la vie privée de différents groupes. Par exemple, vous pourriez effectuer une analyse comparative entre les sexes pour déterminer l'incidence éventuelle des politiques, des programmes et des initiatives sur divers groupes de femmes, d'hommes et de personnes non binaires du point de vue de la vie privée.* ».

Le débat autour du nombre de lignes et de colonnes est sans fin entre experts de la gestion des risques[40]. Pour les tenants de la première approche, un nombre pair évite de tout positionner dans les valeurs médianes et force le choix du répondant. Avec sa modalité impaire, il est vrai que les parties prenantes sont tentées d'opter très souvent pour un avis médian (l'effet « eau tiède »). Ce risque est particulièrement élevé dans des matrices qui ne comportent qu'un faible nombre de lignes et de colonnes. Il faut considérer cela comme un biais potentiel : la modalité neutre peut constituer un choix refuge et concentrer une majorité des réponses. Dans ce cas, les évaluations risquent de ne pas être significatives et la pertinence de l'AIPD d'être remise en cause.

Naturellement, un nombre plus élevé de lignes et de colonnes permet d'obtenir des données plus nuancées et permettent de minimiser le biais évoqué *supra* : c'est la raison pour laquelle je trouve peu pertinentes les matrices 3x3 (pourtant utilisées, par exemple, par l'ICO - *Information Commissioner's Office*).

Il convient également de déterminer le type des échelles utilisées sur les deux axes (et si elles vous sont imposées par un outil, de comprendre leur nature). Elles peuvent être ordinales ou quantitatives et cela dépend de la méthode utilisée pour évaluer les risques. Dans une échelle ordinale (la plus fréquemment observée dans les AIPD), les risques sont classés par rang (par ordre). Le nombre éventuellement associé à chaque rang (ou niveau) indique uniquement un rang et pas une quantité. Ainsi, un risque positionné dans la ligne de rang 4 n'est pas deux fois plus « grand » qu'un autre figurant dans la ligne de rang 2. Ce type d'échelle indique seulement que le premier risque est plus important que le second (on s'en sert uniquement pour évaluer la gravité des risques les uns par rapport aux autres). Il n'existe alors aucune cohérence ni progressivité régulière entre les niveaux[41]. Il faut alors faire attention à la valeur des écarts entre chaque rang car, à défaut, ce type d'échelle peut déboucher sur des conclusions erronées. Ainsi l'exemple suivant[42] me laisse dubitatif. Il s'appuie sur des échelles de quatre valeurs. Ainsi, l'échelle de gravité comporte les niveaux « *Limité = Presque aucun impact* », « *Significatif = Impact peu conséquent* », « *Critique = Conséquence(s) importante(s)* » et « *Catastrophique = [Allant jusqu'au] Danger de mort* ». Personnellement, je trouve des écarts inégaux entre ces quatre valeurs, avec notamment un véritable gouffre entre « *Significatif* » et « *Critique* ». De plus, je trouve le terme « *Significatif* » peu en rapport avec la définition proposée (« *Impact peu conséquent* »). Il aurait sans doute fallu opter pour une échelle avec 5 barreaux (permettant une plus grande nuance et une meilleure progressivité entre les niveaux) et mieux choisir les termes (et les définitions) associés à chacun d'entre eux.

Dans une échelle quantitative, chaque risque est affecté sur chaque axe d'un nombre compris entre 0 (« *Cela ne se produira certainement pas* » par exemple concernant la vraisemblance) et 1 (« *Cela se produira certainement* »), et toutes les valeurs intermédiaires sont possibles. Certains vont jusqu'à envisager d'écarter totalement l'humain grâce à ce type d'approche, comme Luis Enríquez qui s'exprimait sur l'utilisation du modèle FAIR[43] sur les risques liés à l'IA lors de la conférence FAIR 2023 : « *Je considère que les DPO et les RSSI ne sont ni des juges ni des autorités administratives, et qu'ils ne disposent pas de la formation et des compétences nécessaires pour prévoir l'impact sur les droits et libertés des personnes physiques. Dès lors, comment peuvent-ils estimer l'impact d'un traitement de données sur les personnes concernées ? Pour bâtir ma solution Pd-VaR[44] (Personal Data Value at Risk), j'ai utilisé l'étude*

[40] Voir par exemple le passage suivant qui figure dans le document « Le supplément » associé à la méthode EBIOS (Anssi) en page 14 : « *L'usage d'une échelle à 4 ou 5 niveaux est guidé par les considérations suivantes : la nécessité de mesurer des impacts très élevés qui correspondent à des crises majeures, voire une déstabilisation et une perte de résilience allant au-delà de la seule organisation concernée. Dans ce cas, une échelle à 5 niveaux est recommandée. Dans le cas contraire, 4 niveaux suffiront.* ». À noter que le standard MIL-STD-882B utilise une matrice 4x5 (*Severity x Probability*).

[41] Le papier suivant évoque d'autres biais possibles : *Problems with Risk Matrices Using Ordinal Scales*, Michael Krisper, Institute of Technical Informatics Graz University of Technology (Austria), march 2021

[42] Exemple trouvé sur le site macartodesrisques.fr, une plateforme gratuite dédiée aux PME et ETI, développée par l'Amrae et le Medef Deux-Sèvres, qui permet de réaliser un autodiagnostic et une cartographie des risques (pour les entreprises) en quelques clics.

[43] *Factor Analysis of Information Risk*

[44] Voir le papier *A Personal Data Value at Risk (Pd-VaR) approach*, par Luis Enríquez, November 5, 2024

scientifique du système juridique et l'analyse prédictive de la protection des données pour mettre en œuvre des modèles de recherche à partir de données historiques tirées des sanctions administratives publiées. Cela m'a aidé à établir le profil de la "psychologie des sanctions" des régulateurs et à obtenir des données à partir de leurs raisonnements juridiques. J'ai ensuite fusionné ces données avec l'état actuel de maturité en matière de conformité basée sur les risques d'un responsable du traitement des données. Mes premières implémentations étaient basées sur le modèle FAIR, mais j'ai été obligé de l'adapter au RGPD. ».

De l'importance de la sémantique

L'axe de vraisemblance de la représentation proposée par l'outil PIA de la CNIL comprend les valeurs suivantes : négligeable, limitée, importante et maximale. On retrouve cette même sémantique pour qualifier les niveaux de gravité. J'avoue que cette similitude me gêne[45]. Il me semble que l'utilisation de termes plus adaptés à chaque composante du risque serait plus pertinente. Je prends pour exemple la sémantique qui figure dans l'un des exemples fournis par l'EDPS dans la figure 12 de son document *Report on DPIA survey 2024 to EU institutions, bodies, offices and agencies*. Chaque axe comprend ici cinq niveaux. Pour la vraisemblance, on trouve les valeurs « *Rare* », « *Peu probable* », « *Possible* », « *Probable* » et « *Presque certain* ». Concernant la gravité, les échelles sont « *Très faible* », « *Faible* », « *Moyenne* », « *Élevée* » et « *Très élevée* ». Dans un autre document, la CNIL mentionne une sémantique bien mieux adaptée : « *Improbable* », « *Occasionnel* », « *Courant* », « *Très courant* » (pour la vraisemblance) et « *Indolore* », « *Limité* », « *Grave* » et « *Dramatique* » (pour la gravité). À titre de comparaison, je signale les termes utilisés dans la matrice de cotation de la norme qui est à l'origine de la méthode AMDEC concernant la sévérité (gravité[46]) : « « *Mineur* », « *Marginal* », « *Critique* » et « *Catastrophique* ». On comprend bien que le choix des expressions peut avoir un effet sur le lecteur de l'AIPD, qui réagira sans doute d'avantage à la vue d'un risque coté « *Catastrophique*[47] » plutôt que « *Maximal* ».

On peut pousser le raisonnement plus loin et chercher une plus grande appropriation par les parties prenantes à l'AIPD (et une meilleure compréhension par le responsable de traitement), en utilisant une sémantique encore plus proche du langage parlé, comme on l'observe dans la méthode Kinney-Wiruth[48] dont l'échelle de vraisemblance comporte sept niveaux : « *C'est virtuellement impossible*[49] », « *C'est pratiquement impossible* », « *C'est concevable, mais très improbable* », « *C'est tout juste possible* », « *C'est inhabituel mais possible* », « *C'est tout à fait possible* » et « *On peut s'y attendre, c'est certain* ». Enfin, si la méthode retenue prend en compte un troisième axe, celui de la « détectabilité » (ou « maturité »), il convient également d'en déterminer soigneusement la sémantique. Ainsi, dans cet exemple, il est proposé les valeurs suivantes (du meilleur au pire) : « *Contrôle proactif (alertes)* », « *Contrôles en place* », « *Contrôles réguliers* » et « *Aucun contrôle* ».

La question de la définition des échelles de cotation

Au-delà de l'attention qu'il convient d'apporter à la sémantique utilisée, il faut également objectiver chaque valeur des échelles de cotation[50]. Au sein des nombreuses AIPD que j'ai eu l'occasion de lire, on en trouve

---

[45] On la retrouve aussi dans la norme ISO 29134 (Lignes directrices pour l'étude d'impacts sur la vie privée), qui utilise les termes suivants (et identiques pour les deux axes) : Négligeable, Limité, Signifiant, Maximum.

[46] Voir également la sémantique relevée dans le document *Privacy Impact Assessment toolkit for Health and social care* de *la Health Information and Quality Authority* irlandaise (octobre 2017) : négligeable, mineur, modéré, majeur et critique.

[47] *C'est le terme proposé dans le document « Le supplément » mis à disposition par l'ANSSI concernant la méthode EBIOS-RM pour qualifier le niveau de plus élevé de l'échelle de gravité (voir page 15).*

[48] *KINNEY G. F. and WIRUTH A. D. (1976) Practical Risk Analysis for Safety Management, NWC Technical publication 5865, Naval Weapons Center, China Lake, CA*

[49] Ce niveau (rencontré très rarement) permet de positionner des risques tels que l'attentat du 11 septembre 2001, le tsunami de Fukushima, le blocage du canal de Suez ou la pandémie de COVID 19. Dans son essai « *Le Cygne noir : la puissance de l'imprévisible* », le statisticien Nassim Taleb, développe une théorie selon laquelle on appelle cygne noir un certain événement imprévisible qui a une très faible probabilité de se dérouler et qui, s'il se réalise, a des conséquences d'une portée considérable et exceptionnelle.

[50] Il est recommandé d'illustrer chaque définition par quelques exemples. Ainsi, concernant la gravité, on peut imaginer d'illustrer le premier niveau par la réception de sollicitations publicitaires non sollicitées (c'est à dire des pourriels) et le niveau « *Élevé* » par une interdiction

malheureusement peu souvent une définition objective, ce qui donne l'impression que c'est une étape qui a été oubliée. La plupart du temps, on s'est contenté d'utiliser l'approche embarquée dans la méthode utilisée, sans réellement la connaître ou la maîtriser. Pourtant, certaines méthodes obligent à la réflexion, comme EBIOS RM, qui laisse libre son utilisateur notamment de définir sa méthode d'appréciation de la vraisemblance (en l'axant cependant principalement sur la réalité de succès de l'attaquant). Ainsi, pour la CNIL, en cas de gravité maximale, « *les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter* » - et la Commission de citer le décès de personnes concernées parmi quelques exemples, ce que fait également la norme ISO 29134 : « *Maximum - Données dont la diffusion, la modification, la perte ou la destruction non-autorisée peut affecter l'existence ou la santé, la liberté et la vie des personnes concernées. Les personnes pourraient rencontrer des inconvénients significatifs, voir irréversibles, des conséquences insurmontables* ».

Permettez-moi de revenir sur l'exemple, que j'ai trouvé sur le site macartodesrisques.fr dont je rappelle les niveaux de l'échelle d'évaluation de la vraisemblance : « *Improbable = Cela n'est jamais arrivé et il n'y aucune chance que cela arrive* » ; « *Rare = Cela n'est jamais arrivé et il est peu probable que cela arrive* » ; « *Occasionnel = Cela est arrivé quelques fois et il est probable que cela arrive à nouveau* » ; « *Fréquent = Cela arrive régulièrement et cela va continuer d'arriver régulièrement* [51]». Cette échelle s'appuie sur un passé constaté (donc une sinistralité connue), ce qui est rarement le cas. Et quel est le périmètre retenu ? Uniquement l'organisme qui réalise l'AIPD ou bien on prend un périmètre plus large, en tenant compte de ce qui est arrivé au sein d'autres responsables de traitement[52] ? De plus, l'utilisation du « *et* » sous-entend que les choses sont immuables : si l'événement s'est rarement produit par le passé *alors* il en sera automatiquement de même dans le futur. Est-ce si sûr ? Ces « *et* » ne devraient-ils pas être remplacés par des « *et/ou* » pour englober des évaluations plus réalistes ?

Il suffit d'ailleurs de questionner plusieurs des parties prenantes à l'exercice pour recueillir, pour chaque niveau, des appréciations très différentes (sans compter l'idée que s'en fera le responsable de traitement, qui doit endosser les risques résiduels). Ainsi, dans le rapport d'audit des AIPD réalisées par les DPO des organes européens en 2024 et publié par l'EDPS, on trouve les reproches suivants : « « *Certaines des analyses d'impact auditées ne précisent pas comment elles aboutissent à une note spécifique plutôt qu'à une autre… les critères d'attribution des valeurs à la gravité, à la probabilité et à l'impact restent souvent flous.* », « *Bon nombre de ces AIPD ne fournissent aucune clarification sur la manière dont elles aboutissent à une note numérique spécifique. Cela est regrettable. Il faut aller au-delà du simple cochage de cases et assurer une attribution raisonnée de notes numériques.* ». Dans le rapport d'audit précédent (celui de 2020), on trouvait déjà le conseil suivant : « *Pour mener votre analyse d'impact, vous êtes libre de choisir l'une des méthodologies existantes ou de créer la vôtre, mais pour qu'elle soit pleinement efficace, elle doit au moins comprendre : …/… une méthode permettant d'estimer la probabilité et l'impact de ces événements ; une méthode permettant de calculer les risques pour les personnes concernées en fonction des événements, de leur probabilité et de leur impact.* ». Dans son papier intitulé *Review of the strengths and weaknesses of risk matrices*, Mustafa Elmontsri formule un reproche identique : « *Les positionnements des risques sur la matrice sont soumis à de nombreuses considérations, dont certaines peuvent même échapper à l'évaluateur. Pourtant, et c'est là un problème grave, les explications et justifications requises sont rarement, voire jamais, fournies.* ».

Il est vrai que l'objectivation des échelles de cotation utilisées est un exercice difficile et qui génère de nombreux débats. Un exemple est celui qui peut se tenir lors de l'objectivation de chaque « barreau » d'une

bancaire ou l'usurpation de l'identité. Pour le dernier niveau (« *Très élevé* » voire « *Dramatique* »), on peut évoquer le divorce, le suicide ou un handicap sévère.

[51] Il convient de chercher, dans les définitions de chaque niveau, à expliciter les fréquences correspondantes. Dans ces exemples, que signifient « *quelques fois* » et « *régulièrement* » ?

[52] Dans l'un des exemples d'analyse de risques (et non pas d'impact) publiés par le Club EBIOS, la définition du niveau le plus élevé de vraisemblance (« *4. Certain ou déjà produit* ») répond à cette question : « *Un tel scénario s'est déjà produit au sein du Club EBIOS ou d'autres associations analogues* » (Cf. Page 17).

échelle de cotation de gravité : le nombre de personnes éventuellement concernées par l'événement redouté doit-il être retenu comme critère pertinent ? Ainsi, un document émanant de l'Université Monash (Australie) prend en compte, parmi les critères permettant de le déterminer un impact mineur, le « *petit nombre de personnes affectées* ». De même, la méthode PRAM (*Privacy Risk Assessment for Data Subject Aware Threat Modeling*) tient compte du nombre d'éventuelles victimes pour déterminer la gravité associée à un risque. Pour ma part, même s'il n'y avait qu'une seule personne concernée, l'appréciation de l'impact du risque ne devrait pas tenir compte de ce facteur dans le cadre d'une AIPD. Pour une victime, le fait qu'elle soit seule à souffrir des conséquences d'un traitement de données personnelles (ou qu'elle en souffre aux côtés d'autres personnes) n'a que peu d'importance.

Quel choix de couleurs ?

Les couleurs appellent des émotions fondées sur des expériences communes, profondément ancrées dans chaque culture. Alors qu'en Chine, le rouge est la couleur de la chance et de la prospérité, en occident il évoque des émotions intenses comme la passion, la colère, le danger, probablement parce que c'est la couleur du sang. *A contrario*, la couleur verte nous transmet un sentiment de sérénité puisqu'elle rappelle la nature (et nous donne liberté de circuler). Ainsi, même sans que nous nous en rendions compte, les couleurs peuvent changer notre perception des choses et peuvent être utilisées pour influencer nos décisions. C'est la raison pour laquelle on doit choisir avec précaution celles qui figureront dans une matrice des risques car elles auront forcément une influence. On doit également veiller à une correspondance pertinente avec la sémantique évoquée *supra* : il serait surprenant d'utiliser la couleur rose pour un risque évalué comme catastrophique !

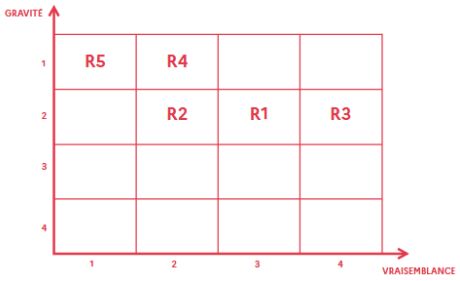


Figure 9 : Exemple "Société de biotechnologie fournissant des vaccins" - ANSSI

Pour commencer, je mets de côté les matrices qui se passent totalement de couleurs – assez rares - comme celle qui figure dans la vidéo de présentation de l'outil PIA de la CNIL ou celle qui figure en page 72 du document « EBIOS Risk Manager – Le guide » de l'ANSSI (Fig. 9). Pourquoi se priver de la charge symbolique des couleurs pour mieux faire prendre conscience au responsable de traitement les enjeux associés au projet de traitement ?

On rencontre rarement des matrices qui ne font intervenir que des nuances d'une même couleur. *A minima*, je rencontre des illustrations faisant intervenir trois couleurs, comme le fait fréquemment l'ICO (au sein d'une matrice 3x3, Fig. 10) ou le NIST (au sein d'une matrice 5x5, tiré du document *Prioritizing Cybersecurity Risk for Enterprise Risk Management* - NIST Interagency Report NIST IR 8286B-upd1 February 2025. Fig. 11).

Severity of impact				
	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Figure 10 : Matrice type utilisée par l'ICO

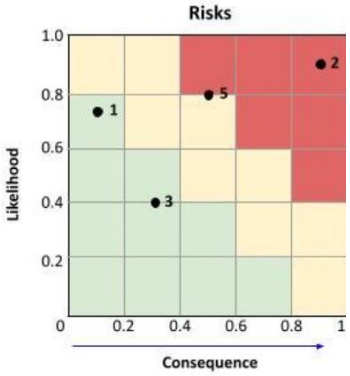


Figure 11 : Matrice type utilisée par le NIST

Bien que ces deux exemples utilisent la même palette de couleurs (rouge pour les risques inacceptables, rose pour les risques maitrisés et vert pour les risques uniquement surveillés), je note une caractéristique qui me semble peu pertinente dans le modèle de l'ICO, en l'occurrence le fait que plusieurs cases vertes soient contiguës à des cases rouges. Comment peut-on passer si rapidement d'une situation extrême à une autre situation extrême ? Le modèle du NIST évite cette violation de l'une des règles qui devraient s'imposer (Deux cases « extrêmes » ne devraient jamais se toucher mais être séparées *a minima* par une couleur intermédiaire[53]).

On relève ensuite des matrices qui utilisent un plus grand nombre de couleurs, cinq par exemple dans le modèle utilisé à Singapour[54] (Fig. 12). Le maximum que j'ai relevé dans les analyses d'impact RGPD que j'ai eu l'occasion de consulter est de sept. Il me semble qu'il ne faudrait pas aller au-delà de quatre à cinq couleurs, mais je n'ai trouvé aucune étude pertinente à ce sujet.

IMPACT						
	Very Severe (5)	Medium (5)	Medium High (10)	High (15)	Very High (20)	Very High (25)
	Severe (4)	Low (4)	Medium (8)	Medium High (12)	High (16)	Very High (20)
	Moderate (3)	Low (3)	Medium (6)	Medium (9)	Medium High (12)	High (15)
	Minor (2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium High (10)
	Negligible (1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)
		Rare (1)	**Unlikely (2)**	**Possible (3)**	**Likely (4)**	**Highly Likely (5)**
				LIKELIHOOD		

Figure 12 : Modèle du Cyber Security Agency of Singapore (CSA)

Alors que je l'ai moi-même utilisée dans le cadre de mes premières AIPD, j'avoue avoir cessé d'utiliser la couleur verte dans une matrice des risques RGPD[55], car, culturellement, elle véhicule le message selon lequel il n'existe aucun risque… ce qui est faux[56]. De plus, la zone habituellement colorée ainsi (généralement le carré situé en bas à gauche, avec des notes de vraisemblance et de gravité faibles) est souvent accompagnée du commentaire suivant : « *Aucune mesure n'est nécessaire* ».

Pour ma part, la mise en œuvre d'une mesure de détectabilité me parait *a minima*, indispensable, ne serait-ce que pour constater la pertinence des évaluations (Ces risques sont-ils aussi rares qu'escomptés ?) et pour être éventuellement en mesure de revoir sa copie. Je note que, dans son document *Risikoanalyse und Datenschutz- Folgenabschätzung*, le délégué bavarois à la protection des données montre une matrice des risques 4x4 (Fig. 13) qui fait apparaitre trois niveaux de risques, colorés en vert, jaune et rouge. Le texte qui l'accompagne fait bien état de l'existence de risques pour la zone verte : « *En matière de protection des données, l'indice de risque comporte exactement trois niveaux. En effet, le RGPD utilise les termes « risque » et « risque élevé », le terme « risque » pouvant également être qualifié de « risque normal ». En outre, le RGPD utilise*

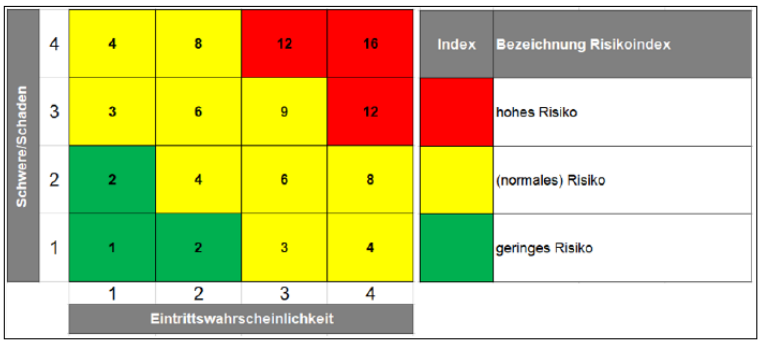


Figure 13 : Matrice recommandée par l'autorité bavaroise

[53] C'est l'une des règles rappelées dans l'article *What's wrong with risk matrices?*, par Louis Anthony Cox Jr (publié en avril 2008 dans la revue *Risk Analysis*)

[54] Cf. *Guide to conducting cybersecurity risk assessment for critical information infrastructure*, *Cyber Security Agency of Singapore* (CSA), 2019

[55] En revanche, je conçois que la couleur verte soit utilisée dans le cadre d'une analyse de risques (pour l'entreprise), pour y placer les risques jugés non prioritaires par la direction.

[56] De façon très surprenante, dans son document *PDB Assessment Methodology*, l'ICO ne voit pas la nécessité d'impliquer le DPO pour les risques figurant dans cette zone !

principalement la formulation « ne devrait pas présenter de risque » (art. 27, al. 2, let. a et art. 33, al. 1 du RGPD). Étant donné qu'il ne peut y avoir de traitement totalement sans risque, l'expression « ne devrait pas présenter de risque » est principalement comprise, compte tenu de son sens et de son objectif, comme « ne présentant qu'un risque faible » ».

J'ai également été surpris d'observer des matrices ou des échelles utilisant des dégradés de couleurs, comme dans l'outil PIA de la CNIL, alors pourtant que les échelles utilisées sont ordinales. Comme il n'est pas possible de positionner le curseur sur une valeur intermédiaire, j'avoue ne pas avoir compris la logique de ce type de représentation.

Figure 14 : Extrait de la vidéo de présentation de l'outil PIA de la CNIL

Représenter une limite d'acceptabilité ?

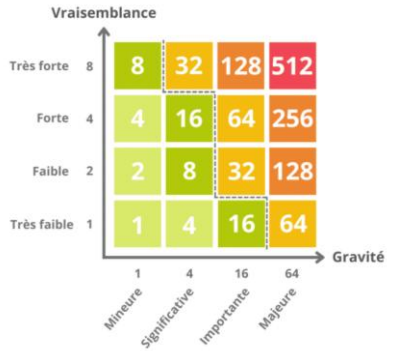


Figure 15 : Une limite d'acceptabilité, deux zones

La limite d'acceptabilité est l'une des notions les plus importantes du management du risque. Elle est généralement représentée par une courbe ou par une ligne, et divise la matrice au maximum en trois zones distinctes : celle des risques inacceptables, celle des risques acceptés et traités et celle des risques acceptés mais uniquement surveillés.

La figure 15 montre un exemple montrant deux zones[57]. On remarquera que toute la ligne correspondant à une gravité majeure est positionnée dans la zone des risques inacceptables, même pour ceux de vraisemblance très faible (attention : les axes sont ici inversés par rapport à la représentation la plus fréquente).

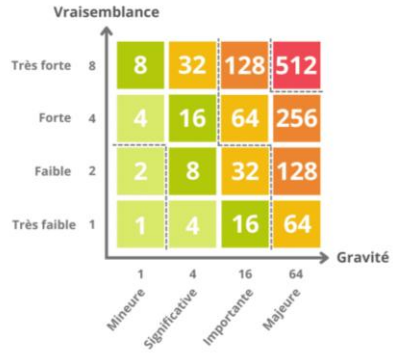


Figure 16 : Trois limites d'acceptabilité, quatre zones

Et voici (Fig.16) la même matrice montrant quatre zones : la case rouge est positionnée en zone « inacceptable » (le domaine interdit). Si un risque net (résiduel) s'y trouve, cela devrait obliger le responsable de traitement à consulter la CNIL au titre de l'article 36 du RGPD[58]. Malheureusement, le document source n'indique pas les décisions associées aux autres zones. On peut imaginer que les risques nets situés dans la première zone intermédiaire devront être traités et surveillés de façon très rigoureuse avant la mise en œuvre du traitement, tandis que ceux situés dans la seconde zone intermédiaire devront être traités et surveillés. Enfin, ceux situés dans la dernière zone (ici, les cases notées 1 et 2) ne demanderaient qu'à être monitorés ?

On voit donc bien les conséquences cruciales du positionnement des limites d'acceptabilité pour le responsable de traitement (et le projet en question) – et les décisions qui sont associées à chaque zone. Selon le positionnement des risques résiduels et des limites d'acceptabilité, l'organisme peut perdre totalement le contrôle du calendrier et dépendre de l'autorité de contrôle (qui peut même aller jusqu'à refuser la mise en œuvre du traitement) dans le cadre de l'article 36 du RGPD.

[57] Source : https://pyx4.com/blog/comment-construire-echelles-de-cotation-des-risques/

[58] Les postures des responsables de traitement peuvent être variées, entre ceux qui veulent avoir le moins souvent possible à faire à la CNIL et ceux qui veulent se couvrir en la sollicitant systématiquement. Le curseur penche du côté du premier cas.

Pour ma part, je regrette qu'une minorité d'AIPD contienne une définition claire et assumée de ces limites (qui devraient être déterminées par le responsable de traitement et ne pas varier d'une analyse d'impact à une autre) : je les vois très rarement figurer dans les matrices alors qu'elle aborde le sujet crucial (« *Le niveau global de risque résiduel nous oblige-t-il à consulter la CNIL ?* »).

On en trouve un exemple (Fig. 17) dans l'une des fiches pratiques dédiées au RGPD et publiée par le Clusif (Club de la sécurité de l'information français). Au chapitre 7. de la fiche PIA, on trouve le passage suivant : « *Un risque résiduel peut notamment être considéré comme élevé et inacceptable dès lors qu'il exposerait les personnes à des conséquences importantes, voire irréversibles, qu'elles seraient susceptibles de ne pas pouvoir surmonter (par exemple : un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière) et/ou lorsqu'il semble évident que le risque se concrétisera (par exemple : dans la mesure où il n'est pas possible de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée).* ».

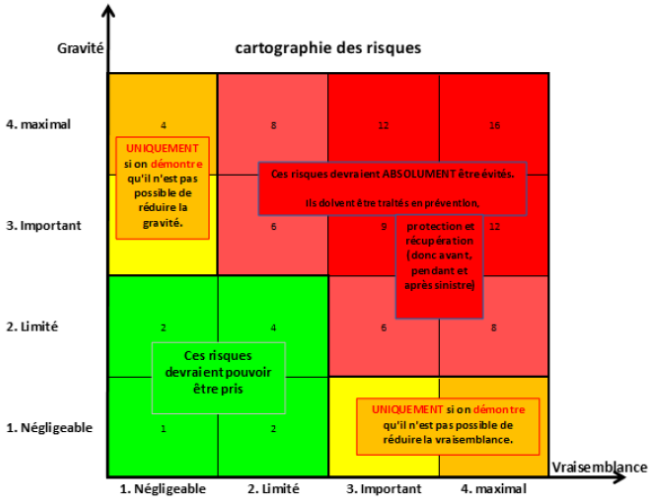
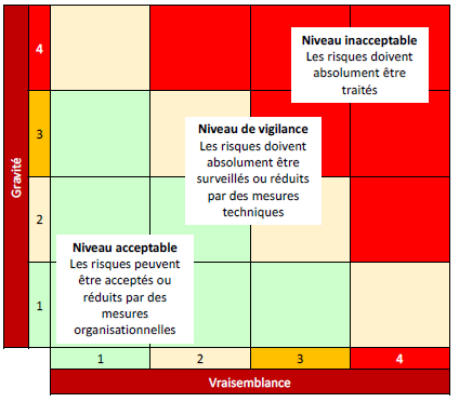


Figure 17 : Exemple de matrice faisant apparaitre clairement les règles qui "déclenchent" l'article 36. RGPD

L'illustration est accompagnée du commentaire suivant : « *Dans le cas où la gravité est importante et la vraisemblance négligeable et dans le cas où la gravité est négligeable et la vraisemblance importante (c'est-à-dire pour les deux carrés orange du schéma), l'organisme doit sérieusement se poser la question d'une consultation de la CNIL* ».



On en trouve une autre occurrence dans l'un des exemples d'étude des risques (et non pas d'impact) publiées par le Club EBIOS (Fig. 18). À l'occasion, on relève les différences énormes qui existent entre les deux matrices (celle du Clusif et celle du Club EBIOS) : alors qu'il s'agit de deux matrices 4x4, on note un choix de couleurs et une répartition de celles-ci totalement différents. À méditer…

Figure 18 : Matrice de décision utilisée par le Club EBIOS

En voici ci-dessous un troisième exemple, issu d'une production du groupe « Données de santé » de l'AFCDP. La matrice de décision (Fig. 19) est accompagnée des définitions suivantes : « *Rouge : Ces risques devraient absolument être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité et leur vraisemblance. Dans l'idéal, il conviendrait même de s'assurer qu'ils sont traités à la fois par des mesures indépendantes de prévention (actions avant le sinistre), de protection (actions pendant le sinistre) et de récupération (actions après le sinistre) ; Orange : Ces risques devraient être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité ou leur vraisemblance. Les mesures de prévention devraient être privilégiées. Ils peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur gravité et si leur vraisemblance est négligeable ; Jaune : Ces risques devraient être réduits par l'application de mesures de sécurité diminuant leur vraisemblance. Les mesures de récupération devraient être privilégiées. Ils peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur vraisemblance et si leur gravité est négligeable ; Vert : Ces risques devraient pouvoir être pris, d'autant plus que le traitement des autres risques devrait également contribuer à leur traitement.* ».

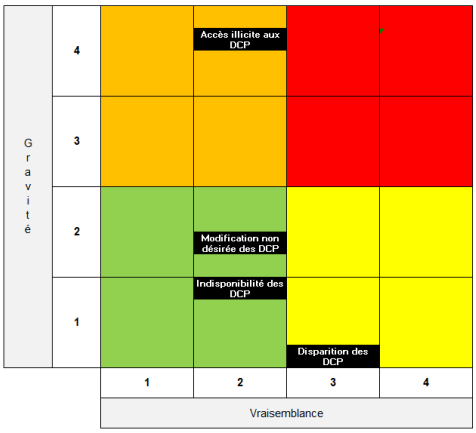


Figure 19 : Matrice de décision du groupe "Données de santé" de l'AFCDP

Sur cet exemple précis, j'ai émis trois réflexions auprès du confrère DPO qui a piloté les travaux : 1) Comme je l'ai indiqué *supra*, j'ai un avis différent concernant l'utilisation de la couleur verte et des « non décisions » qui y sont associées ; 2) Je reste dubitatif quant à l'utilisation de la couleur jaune pour toutes les cases de la ligne supérieure, puisque cette même AIPD précise que ce niveau correspond à des risques *irrémédiables* (c'est à dire, potentiellement, la mort de personnes concernées). Avec les définitions objectivées, n'aurait-il pas fallu conseiller au responsable de traitement de consulter la CNIL au titre de l'article 36 du RGPD (alors que cette matrice permet de « passer sous le radar » ... en faisant porter des risques dramatiques sur les personnes concernées) ? Enfin je m'interroge également sur l'évaluation de la gravité liée à une indisponibilité des données de santé (ici évaluée à 2 en brut, c'est à dire « *Il semble difficile pour les sources de risques retenues de réaliser la menace*[59] ») en rapprochant cela du décès survenu dans un hôpital britannique à la suite d'une cyberattaque qui a retardé l'obtention de résultats d'analyses et provoqué des reports d'intervention. Le patient est décédé à cause de sa greffe annulée. On rappellera qu'en 2024, le CERT Santé a référencé en France une soixantaine de cas dans lesquels des patients ont été mis en danger du fait d'incidents de sécurité.

Reste que plusieurs consœurs et confrères DPO (internes comme externes) m'ont avoué piteusement définir les couleurs de la matrice et les limites d'acceptabilité après avoir positionné les risques résiduels, de façon à satisfaire leur responsable de traitement (ou leur client) et éviter la consultation de la CNIL au titre de l'article 36 du RGPD[60]. Outre que cela témoigne d'une qualité déplorable de l'AIPD produite, cela constitue autant de bombes à retardement qui risquent de poser problème à leurs auteurs si l'autorité en prend connaissance, par exemple à l'occasion d'un contrôle.

La matrice permettrait de prioriser les mesures : vraiment ?

Très fréquemment, dans la littérature associée à la gestion des risques, on relève que la matrice permettrait « *de prioriser les actions en fonction du niveau de gravité identifié pour chaque risque* ». Si cette affirmation a un sens dans

[59] On voit ici le danger de restreindre l'évaluation de la vraisemblance à un seul facteur, ici la « facilité » avec laquelle la source de risque va matérialiser l'incident.

[60] Cas extrême, quand le responsable de traitement commet un faux en écriture en modifiant l'avis qu'avait donné son DPO (qui, de négatif, devient très positif), à l'insu de ce dernier. Cf. *Il faut sauver le soldat DPO !*, page 17, Bruno Rasle, 5 mai 2023

le cadre d'une analyse de risques - ceux pesant sur un organisme, qui décide en pleine conscience d'accepter des menaces qui pèsent sur lui et qui peut étaler dans le temps la mise en œuvre des mesures de traitement – cela n'en a à mon avis aucun dans le cadre d'une analyse d'impact RGPD, ne serait-ce que parce que les mesures doivent être implémentées *avant* la mise en œuvre du traitement[61]. Et concernant l'allocation efficace des ressources pour faire face aux menaces, le diagramme d'Ishikawa[62] (en arêtes de poisson) donne de meilleures possibilités d'identifier là où il faut porter son effort.

L'affirmation fait également difficilement sens quand on voit des matrices qui utilisent la même couleur pour des cases dont la multiplication des évaluations en vraisemblance et gravité donnent le même résultat suivant la formule fréquemment utilisée $R_{(Risque)} = V_{(Vraisemblance)} \times G_{(Gravité)}$. En effet, l'appréciation du risque n'est pas linéaire en fonction de chacune des deux variables et cette notion doit être utilisée avec prudence car chacun comprend bien qu'un événement redouté ayant une vraisemblance de 5 et une gravité de 1 ne devrait pas être perçu de la même façon qu'un événement ayant une vraisemblance de 1 et une gravité de 5. Le sens commun incite à porter son effort sur le second cas (dans lequel le traitement va peut-être provoquer le décès d'une personne concernée) plutôt que sur le premier (qui ne débouchera que sur des nuisances pour ceux qui en seront les victimes). Cette remarque devrait nous inciter à utiliser une couleur plus « alarmante » pour toutes les cases correspondant à une gravité maximale.

Si – dans le cadre d'une AIPD- les matrices traditionnelles ne nous aident donc pas à prioriser la mise en œuvre des mesures de traitement des risques (évitement ou réduction des impacts), elles peuvent toutefois être utiles pour identifier les risques qui nécessitent une supervision accrue (en clair, ceux qui doivent être surveillés « *comme le lait sur le feu* »). En l'occurrence, si l'on reprend l'exemple évoqué *supra*, il serait prudent de positionner des alertes et de réaliser des vérifications régulières pour être en mesure de détecter le plus rapidement possible la survenance des événements redoutés de type V1/G5. Il serait illogique d'être démuni d'une fonction de détectabilité[63] des événements. Dans le cadre de mes enseignements, je recommande, en face de chaque événement redouté, que la question suivante soit étudiée formellement : « *Sommes-nous/Serions-nous en capacité de détecter sa survenance ?* ». Si la réponse est négative, le plan d'action soumis à la signature du responsable de traitement devrait obligatoirement comprendre la mise en œuvre d'une traçabilité (comme la CNIL le rappelle très fréquemment dans ses délibérations[64]) et d'une procédure efficace d'exploitation de celle-ci, y compris de façon synchrone (et non pas seulement en *post-mortem*[65]). Par précaution, on vérifiera régulièrement que la détectabilité reste opérationnelle, pour ne pas se retrouver dans la situation de la société Free Mobile dont la défense, lors du passage le 15 décembre 2025 devant la

---

[61] Dans certains cas, des mesures complémentaires peuvent toutefois être déployées après la mise en œuvre du traitement, du moment qu'elles ne sont pas nécessaires pour réduire un risque à un niveau net acceptable. À titre d'exemple : il a été décidé de réduire la durée de conservation des données personnelles traitées afin de réduire l'exposition aux risques. Lors de la formalisation de l'AIPD, il a été souhaité d'implémenter une purge automatique afin d'alléger la charge induite. Par manque de temps (et/ou de budget), cette mesure n'a pas pu être déployée. Le traitement a donc été mis en œuvre avec une purge manuelle et supervisée. L'AIPD qui a été soumise à la signature du responsable de traitement comprend l'engagement d'enrichir le traitement de cette fonction de purge automatique dès l'exercice budgétaire suivant.

[62] Le diagramme de causes et effets, ou diagramme d'Ishikawa, ou diagramme en arêtes de poisson, est un outil développé par l'ingénieur japonais Kaoru Ishikawa en 1962 et utilisé notamment en gestion de la qualité.

[63] La détectabilité des risques fait référence à la capacité d'une organisation à identifier et analyser les risques auxquels elle est exposée. Cette variable est également appelée « Niveau de maîtrise » dans certaines méthodes.

[64] Cf. par exemple, le passage suivant dans sa délibération n° SAN – 2025-015 du 22 décembre 2025 prononçant une sanction pécuniaire à l'encontre de la société NEXPUBLICA FRANCE : « *… l'impossibilité pour la société d'indiquer quelles données ont fait l'objet des violations met en lumière une traçabilité inefficiente des actions effectuées sur le [traitement]. La formation restreinte rappelle à ce titre qu'il est recommandé de prévoir une traçabilité " active ", c'est-à-dire de formaliser un processus permettant de générer des alertes et de les traiter en cas de suspicion de comportement anormal (voir en ce sens la délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation).* ».

[65] En voici deux exemples concrets de mesures de détectabilité qui réduisent les risques : De nombreux véhicules sont équipés d'une alarme qui signale au conducteur que l'un des pneumatiques est dégonflé, ce qui permet d'éviter des accidents ; l'installation d'un détecteur de fumée et/ou de CO2 est requis dans de nombreux appartements (En dernière estimation, cette obligation aurait permis de sauver quatre cents vies par an en France depuis son entrée en application).

formation restreinte de la CNIL, indiquait que son client était bien doté d'un dispositif de détection des comportements malveillants, mais que celui-ci a été neutralisé à l'occasion d'une montée de version. Il existe d'ailleurs des méthodes de gestion de risques qui intègrent cette dimension de détectabilité en sus de celle de vraisemblance et de gravité (un événement non détectable recevant une note élevée, ce qui augmente le niveau de risque calculé selon la formule $R_{(Risque)} = V_{(Vraisemblance)} \times G_{(Gravité)} \times D_{(Détectabilité)}$), dont la plus connue est la méthode AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité), méthode élaborée par l'armée américaine dans les années 1940.

Tentons de formuler quelques conseils

Au fil de mes recherches, de mes échanges avec mes pairs et de mes réflexions, j'en suis arrivé à dégager quelques conseils destinés à mes consœurs et confrères DPO :

1. **Ton rôle de garant méthodologique tu assumeras :** Dans ses lignes directrices sur le DPO[66], le G29 recommande que le responsable du traitement demande conseil à son délégué notamment sur la méthodologie à suivre lors de la réalisation d'une analyse d'impact relative à la protection des données. Outre le fait de vérifier que le résultat produit répond aux exigences listées dans l'annexe 2 des lignes directrices sur l'AIPD, tu dois sélectionner la méthode apte à fournir un résultat de qualité et dont tu maîtrises les qualités comme les biais[67], que tu sais corriger. Veille également à documenter la procédure utilisée dans tes AIPD ou dans une procédure. Si la réalisation des AIPD est confié à un prestataire extérieur, tu t'informes de la méthodologie qui sera suivie et t'assures de sa pertinence[68].

2. **Ton AIPD, après l'avoir décidé, tu illustreras :** N'insère pas une matrice de risques dans ton analyse d'impact par convention, par habitude ou par mimétisme, mais parce que tu l'as décidé, après avoir clarifié les objectifs que tu souhaites atteindre.

3. **La méthode de conception de ton illustration tu maîtriseras :** De nombreuses AIPD sont produites automatiquement par des outils destinés aux DPO, principalement sur la base d'une série de cases à cocher. S'il s'agit sans conteste d'une aide fort pratique pour les praticiens débutants, il est indispensable que tu t'intéresses à ce qui se cache sous le capot et prennes connaissance de l'algorithme qui t'est imposé par l'éditeur. En connais-tu les principes, les limites et les biais ? Sauras-tu expliquer à ton responsable de traitement pourquoi la vraisemblance et la gravité d'un événement redouté sont évalués à tels niveaux (ou seras-tu obligé d'avouer que tu n'en sais strictement rien ?) ?

4. **De la valeur ton illustration créera :** Si la matrice n'ajoute rien à l'analyse d'impact soumise au responsable de traitement, c'est qu'elle est inutile. Si tu insères une illustration, c'est qu'elle doit servir un (ou plusieurs) objectif(s) et créer du sens, de la valeur[69].

---

[66] WP 243, révisée et adoptée le 5 avril 2017

[67] Voir, par exemple *Some limitations of qualitative risk rating systems*, par Louis Anthony Tony Cox Jr, Djangir Babayev et William Huber (publié en juin 2005 dans la revue *Risk Analysis*)

[68] Dans le document *Survey on Data Protection Impact Assessments* publié par l'EDPS en juillet 2020, au chapitre « *DPO involvement - How does the DPO get involved?* », je relève le passage suivant : Lorsque les AIPD *sont sous-traitées à des prestataires externes, il existe un risque que ces derniers ne disposent pas des connaissances et de l'expertise requises et que l'AIPD ne puisse être menée à bien. Nous avons par exemple constaté que certains professionnels, forts de leur expérience en matière d'évaluation de la sécurité informatique, sont convaincus de pouvoir réaliser une AIPD. Cependant, cela n'est pas garanti, car l'expérience montre qu'ils rencontrent des difficultés en raison du manque de compétences appropriées en matière de protection des données.* ».

[69] Je recommande vivement la lecture d'un billet d'humeur décapant mais qui incite à la réflexion, intitulé *Faire une vraie analyse des risques cyber : guide critique d'un professionnel de terrain*. Damien Peschet y égratigne gentiment ces « *matrices rassurantes* ». Extrait choisi : « *Difficile de trouver un symbole plus universel de l'analyse de risques que la matrice à deux axes. En réunion, c'est un outil redoutable : visuel, synthétique, facile à comprendre. Une seule diapositive suffit à montrer qu'on a mesuré les menaces et que l'on sait où concentrer les efforts. Ce pouvoir de simplification est aussi son principal défaut. La matrice crée une impression d'objectivité qu'elle n'a pas. Les chiffres qui*

5. **Honnête ta démarche sera :** L'illustration que tu décides d'insérer dans ton analyse d'impact correspond à une démarche positive, celle d'aider le responsable de traitement à prendre la « bonne » décision en connaissance de cause, et non pas à essayer de masquer, d'amoindrir ou de présenter sous un jour plus avenant des éléments négatifs, ni d'essayer d'influencer la décision. Le métier de DPO est souvent assimilé à un sacerdoce, cela ne peut se faire qu'avec un cœur pur…

6. **Documentée et expliquée ton illustration sera :** Veille à fournir systématiquement (en annexe de l'analyse d'impact si besoin) le « mode d'emploi » de la matrice de risques que tu as décidé d'intégrer : Que signifie chaque degré des échelles utilisées en gravité et vraisemblance ? Quelle méthode a été suivie pour positionner chaque risque sur la matrice ? À partir de quel moment recommandation est faite au responsable de traitement de solliciter l'avis des personnes concernées, voire de la CNIL ? etc. Il faut rester conscient que la matrice *semble* analytique voire scientifique, alors qu'elle ne repose, la plupart du temps, que sur une approche essentiellement subjective, à dire d'experts.

7. **À la sémantique, attention tu porteras :** Les mots qui accompagnent ton illustration ont autant d'importance que la structure de celle-ci. En conséquence, choisis-les avec soin afin qu'ils véhiculent une acception partagée par tous et soient cohérents avec la méthode d'évaluation des risques utilisée. De plus, il est de bonne pratique d'inclure des explications ou des exemples illustrant les qualitatifs d'échelles.

8. **À plusieurs itérations si besoin tu procéderas :** Il serait étonnant de parvenir, dès le premier essai, à la « bonne » formule pour réaliser son AIPD et pour l'illustrer, il faut rester humble et être capable de se remettre en question. Tout nouveau processus comporte ses propres bizarreries et problèmes qui ne peuvent être résolus que par une amélioration continue. Lance toi puis itère, en prenant soin après chaque analyse d'impact de la revoir avec un œil critique (Essaye de te placer comme un observateur extérieur, de prendre du recul).

9. **À la pérennité de ta matrice tu veilleras :** Quoi de plus déroutant qu'une matrice qui varie à chaque analyse d'impact ? Une fois que tu as déterminé la formule qui te correspond (et qui fait consensus), tiens-toi y. Et si d'aventure il est décidé de faire réaliser quelques analyses d'impact par un prestataire, veille à ce que les livrables qui seront produits ne sont pas trop éloignés de l'aspect auquel tu as habitué ton responsable de traitement.

10. **Aux personnes concernées, ton illustration tu présenteras :** Si la matrice des risques était présentée aux personnes directement concernées ou à leurs représentants, qu'elle pourrait être leur réaction ? Comprennent-elles l'illustration sans avoir besoin de vos explications ? Partagent-elles les qualifications qui ont été retenues pour chaque risque ? Refusent-elles de courir (à cause du traitement) des risques qualifiés d'acceptables dans l'analyse d'impact ? Cet effort est d'autant plus utile si ton responsable de traitement est obligé de solliciter la CNIL dans le cadre de l'article 36 du RGPD, la Commission allant sans doute demander « *Et qu'en pensent les personnes concernées ?* ».

---

positionnent un risque sur la grille sont presque toujours le fruit d'estimations subjectives, influencées par la perception des participants, par leur expérience passée, ou par les exemples récents qui leur viennent à l'esprit. Deux équipes différentes, travaillant sur le même périmètre, peuvent obtenir des matrices radicalement différentes. Le résultat, c'est un outil séduisant qui rassure sur la forme mais qui, mal utilisé, entretient un faux sentiment de contrôle. Une matrice bien présentée peut convaincre un comité de direction, démontrer qu'une organisation est en maîtrise, alors même que ses défenses réelles sont incomplètes ou obsolètes. Ce vernis visuel est parfois plus dangereux qu'une absence totale d'analyse, car il réduit la vigilance au moment même où elle devrait rester en alerte. ».

J'en arrive à quel type de matrice ?

Sur la base de toutes les remarques précédentes, je m'oriente désormais vers une matrice 5x5, avec l'axe de vraisemblance en ordonnée et celle de gravité en abscisse (fig. 20). Outre le fait qu'un cinquième niveau offre plus de finesse dans les évaluations, il permet de positionner les *cygnes noirs* si l'on prend soin de consacrer le premier niveau de l'échelle de vraisemblance à la sémantique « *C'est concevable, mais très improbable* ».

Concernant la sémantique, je préfère le terme de *Vraisemblance* à celui de *Probabilité* (qui sous-entend une analyse des fréquences constatées et véhicule une impression de rigueur scientifique dont la démarche ne peut se targuer) et celui de *Gravité* au mot *Impact* (un impact pouvant être positif). L'axe de Vraisemblance comprendrait les niveaux suivants : « *C'est concevable, mais très improbable* », « *C'est tout juste possible* », « *C'est possible* », « *C'est tout à fait possible* », « *On peut s'y attendre, c'est certain* » - en prenant soin de définir chacune de ses expressions. L'axe de Gravité comprendrait les niveaux suivants : « *Négligeable* », « *Limitée* », « *Significative* », « *Critique* » et « *Dramatique* ». Dans mon rôle de garant méthodologique, je veille à combattre la tendance naturelle à vouloir positionner les risques sur la valeur médiane, notamment en annexant à mon questionnaire Delphi une définition de chacun des termes employés, enrichie d'exemples. Ainsi, le niveau « *Dramatique* » pourrait être ainsi précisé : « *L'événement redouté pourrait s'avérer catastrophique pour les personnes concernées, voire irréversible (allant jusqu'à provoquer indirectement leur décès). Du fait du traitement, les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter.* ».

Figure 20 : Proposition de matrice 5x5

Je prône l'utilisation de trois couleurs, jaune, orange, rouge (en évitant, pour les raisons évoquées *supra*, le vert). Elles sont disposées de façon à ne jamais mettre en contact le jaune et le rouge. Toute la ligne de gravité maximale est colorée en rouge, pour être cohérent avec la définition de ce niveau (« *allant jusqu'à provoquer indirectement leur décès* »). Voici une configuration possible (Fig.20), qui doit de toute façon être travaillée avec les parties prenantes. On notera que la case qui figure en haut à gauche (Vraisemblance minimale/Gravité maximale) est volontairement d'une couleur plus « alarmante » que celle positionnée en bas à droite (Vraisemblance maximale/Gravité minimale), alors que leur produit est identique.

Quelle n'a pas été ma surprise de découvrir dans un guide de l'AEPD[70] - dont j'avais pris connaissance lors de sa publication en 2021- une matrice très similaire à celle à laquelle je parviens ! Mille mercis à Pablo Garrote Crespo, DPO de *Grupo Igualatorio Médico Quirúrgico* (IMQ), de m'avoir signalé cela. Le tableau qui figure en page 97 du document espagnol étant présenté avec les axes inversés, je me permets de la retranscrire ici pour plus de lisibilité (Fig. 21). Vous noterez l'utilisation de quatre couleurs (mais pas de la verte), du respect de la règle visant

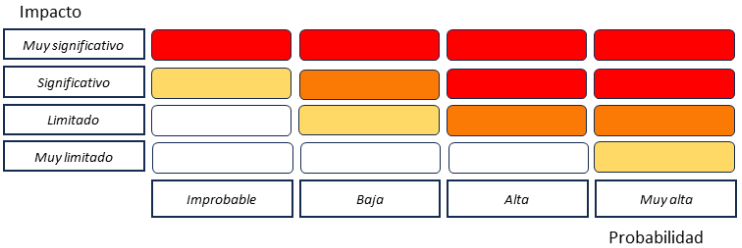


Figure 21 : Tableau tiré du document de l'AEPD

[70] Gestión del riesgo y evaluación de impacto en tratamientos de datos personales, AEPD, juillet 2021

à ce que les couleurs « extrêmes » ne se touchent pas, au fait que l'intégralité de la ligne du haut est en rouge et que les cases en bas à droite et en haut à gauche ne sont pas colorées de la même façon.

Il reste ensuite, après échange avec le responsable de traitement, à positionner les limites d'acceptabilité afin de définir trois zones (Voir un exemple en Fig. 22). La zone 1 est dite zone *interdite* : aucun risque résiduel ne devrait s'y trouver. À défaut, une itération supplémentaire est à réaliser pour ajouter des mesures de traitement ou renforcer l'efficacité des mesures déjà imaginées.

Si, malgré cela, des risques y figurent encore, la CNIL doit être consultée au titre de l'article 36 du RGPD[71]. L'AIPD qui sera fournie à l'autorité sera accompagnée 1) d'un argumentaire démontrant qu'il n'existe pas d'autres approches permettant d'atteindre la finalité et qui présente un niveau de risque inférieur pour les personnes concernées ; 2) de la démonstration de la valeur ajoutée, de l'apport sociétal et/ou du gain pour les personnes concernées créés[72] pour [la société/la communauté/les personnes concernées] ; 3) de la synthèse de l'avis des personnes concernées ou de leurs représentants, comme le prévoit l'article 35.9 du RGPD. Si l'autorité autorise la mise en œuvre du traitement, on mettra en œuvre des mesures de surveillance renforcées afin de détecter très rapidement l'éventuelle survenance des événements redoutés situés dans cette zone. Les risques résiduels positionnés en zone 2 sont endossés, traités et surveillés. Enfin, ceux situés en zone 3 sont surveillés afin de vérifier que l'évaluation de leur vraisemblance est pertinente. Sans surprise, le débat se concentrera sur les deux cases extrêmes, en haut à gauche et en bas à droite. Il appartient au responsable de traitement de décider si la première est en zone 1 ou en zone 2 et d'assumer son choix (on ne rappellera assez jamais la nécessité de faire signer l'AIPD par le responsable de traitement). Et les personnes qui seraient fréquemment impactées par un événement redouté positionné dans la case en bas à droite peuvent subir un cumul de la gravité (à titre d'exemple, une erreur négligeable mais systématique sur le calcul du salaire va générer un manque à gagner dans la durée ainsi qu'une nuisance psychologique)

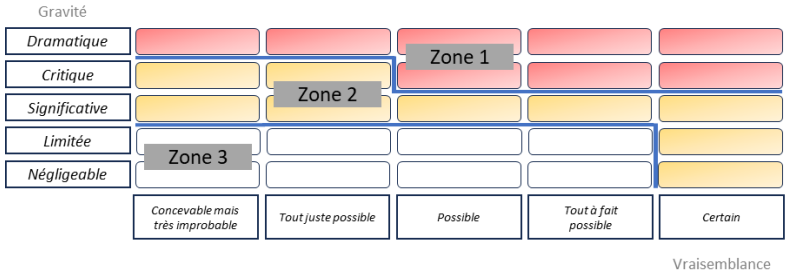


Figure 22 : Ajout des limites d'acceptabilité

La méthode que je me suis forgée pour réaliser des AIPD est fondée sur la méthode de Delphes (que j'ai adaptée), à laquelle j'ai ajouté un zeste de la méthode AMDEC. Plutôt que de représenter chaque risque par un simple rond (noir par exemple s'il s'agit d'un risque brut et bleu pour symboliser le même risque mais en net/résiduel), j'utilise la représentation d'un œil (Fig.23). S'il est fermé, c'est que le responsable de traitement est dans l'incapacité de s'apercevoir de la survenance de l'événement redouté (absence de traçabilité, par exemple). S'il est à semi-ouvert (ou à demi-clos), il existe une traçabilité mais que personne ne consulte. Et s'il est totalement ouvert, le risque sera rapidement détecté (grâce à des alertes ou une exploitation pertinente des informations produites par le dispositif de maîtrise).

Figure 23 : Représentation symbolique du niveau de maitrise de chaque risque

[71] Et préparez-vous à un éventuel contrôle (La CNIL pourrait vouloir vérifier que le traitement n'est pas déjà opérationnel).

[72] Ce concept est imprécis, ce qui ne facilite pas la décision des responsables de traitement. Dans un atelier délivré en 2019 par des agents de la CNIL auprès des membres de l'AFCDP pour présenter l'outil PIA, il nous avait été indiqué ceci : « *Par exemple, on peut prendre certains risques si le traitement permet de sauver des vies humaines. Quels en sont les avantages pour les personnes et ses apports pour la communauté ? La réponse à ces questions permet d'établir un bilan et de savoir si les risques résiduels sont acceptables. Il faut trouver un équilibre entre les risques résiduels et les enjeux du traitement. Dès que l'équilibre penche du bon côté, le PIA peut être validé par le responsable de traitement, avec acceptation des risques résiduels.* ».

Cela me permet de conserver une illustration à deux dimensions de caractère synthétique (Fig.24).

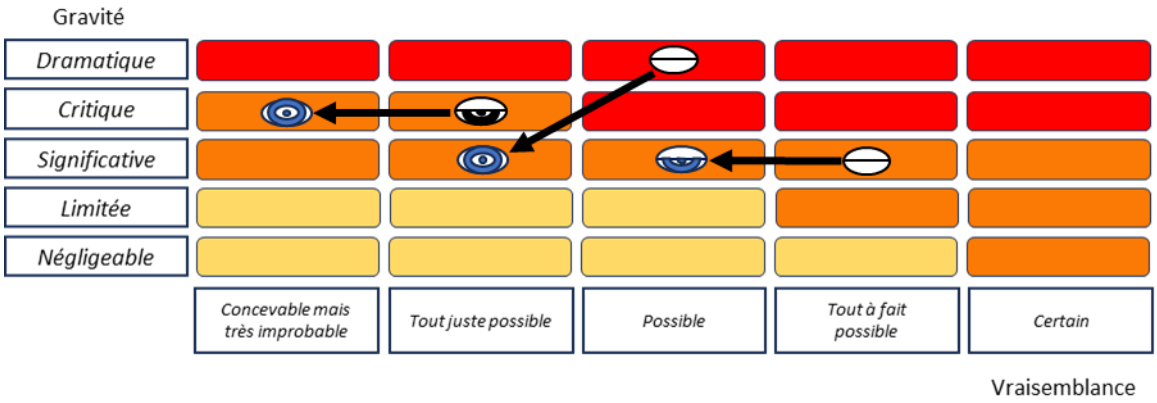


Figure 24 : ma proposition de matrice des risques, enrichie du degré de "maîtrise" de chaque risque.

Un appel lancé aux éditeurs d'outils

Nul n'a été surpris de voir les éditeurs d'outils RGPD (focalisés à l'origine sur la tenue du registre des traitements) enrichir leur offre d'une section permettant aux utilisateurs de formaliser une AIPD. Fort logiquement, ils ont tous intégré la méthode proposée par la CNIL (et matérialisée dans l'outil gratuit PIA mis à disposition par la Commission), avec tous ses avantages mais surtout ses inconvénients. Pour avoir pris soin d'échanger avec plusieurs acteurs majeurs, j'ai noté que ceux-ci avaient cependant décidé de gommer l'un des défauts que présente la représentation graphique des risques de l'outil PIA, notamment en délimitant nettement chaque case de la matrice. L'un d'eux est allé plus loin, en optant pour une sémantique propre pour l'axe Vraisemblance (mais il a conservé celle de l'axe Gravité). Tous ont fait leur propre choix en ce qui concerne les couleurs, mais surtout leur disposition - avec des différences énormes : chaque éditeur impose donc au DPO *sa* doctrine concernant les limites d'acceptabilité, ce qui me parait inconcevable. Tous m'ont indiqué avoir suivi cette logique afin d'aider les nouveaux DPO, principalement ceux éloignés de la chose technique (l'approche étant focalisée sur les aspects de cybersécurité). Cela se traduit par une litanie de questions hors sol dont les réponses apportées débouchent sur le positionnement de trois risques (et seulement trois) sur la matrice. Ainsi, un DPO qui voudrait lui-même disposer plusieurs risques (par exemple à l'issue d'ateliers EBIOS RM) en est empêché. Si cela aide un DPO débutant (et le rassure sans doute), les effets pervers de ce maternage sont pour moi néfastes, dont les principaux sont : DPO obligé de se conformer à une méthode qui lui est imposée (et qui ne lui convient pas forcément), démarche limitée au seul volet « cybersécurité » - ce qui aboutit à ignorer des risques n'appartenant à aucune des trois familles proposées, DPO qui se retrouve seul à se préoccuper de l'AIPD et à essayer de répondre à la longue liste de questions.

Parmi les éditeurs qui ont accepté de répondre à mes questions (merci à eux pour le temps qu'ils m'ont consacré), je n'ai trouvé que Dastra et Witik pour avoir introduit quelques premiers degrés de liberté et avoir été plus loin que simplement intégrer la logique de l'outil PIA de la CNIL en permettant de personnaliser la matrice « de base ». Dastra permet ainsi que changer la sémantique et les couleurs. De plus, un module optionnel de gestion des risques permet d'aller plus loin, notamment en ajoutant des lignes et des colonnes à la matrice et en créant si besoin des nouveaux types de risques (en sus de ceux touchant à la confidentialité, l'intégrité ou la disponibilité). Witik, dans son module optionnel, n'autorise pas l'ajout de lignes et de colonnes mais permet en sus d'affecter à chaque famille de risque un critère témoignant de la maîtrise du dispositif (c'est-à-dire un troisième axe relatif à la capacité à détecter la survenance de l'événement redouté). Cette souplesse permet d'adapter l'outil à la doctrine que s'est forgée le DPO pour piloter les AIPD plutôt que de l'obliger à se voir imposer un carcan.

Pour répondre aux besoins des DPO expérimentés, j'appelle donc de mes vœux l'enrichissement de ces offres offrant aux praticiens plus de libertés afin qu'elles s'adaptent à leur doctrine propre (le RGPD n'imposant aucune méthode pour formaliser une AIPD, du moment qu'elle répond aux critères d'éligibilité).

Voici les degrés de liberté qui me paraissent souhaitables concernant la matrice de risques :
- Choix du nombre de lignes et de colonnes (je conserverais en revanche la Vraisemblance en abscisse et la Gravité en Ordonnée) ;
- Choix de la sémantique sur les deux axes, et possibilité de personnaliser la définition de chaque niveau ;
- Choix des couleurs (permettant, par exemple, d'échapper à la couleur verte) ;
- Choix de l'affectation de la couleur pour chaque case (et, par conséquence, maîtrise des « zones d'acceptabilité », avec personnalisation de la définition de chaque zone) ;
- Possibilité de créer des familles de risques (en sus des trois traditionnelles » relatives à la confidentialité, à l'intégrité ou à la disponibilité) ;
- Possibilité de positionner plusieurs risques dans chaque famille ;
- Et donc possibilité de positionner librement des risques sur la matrice.

« *Une AIPD qui ne comprend pas de matrice est trop facilement mise de côté sans être lue* »

Qu'en pensent nos confrères étrangers ? Plusieurs DPO européens auxquels j'ai adressé une version initiale du présent papier ont accepté de répondre à quelques questions. Voici quelques retours très intéressants :

Utilisez-vous systématiquement une matrice des risques lorsque vous rédigez des AIPD ?

> « *En tant que DPO externe, je travaille principalement avec des PME dont certains mènent des activités de traitement qui nécessitent une AIPD, comme la vidéosurveillance ou des activités de profilage/d'analyse dans le secteur du tourisme. Au sein de ces analyses, j'intègre généralement une matrice des risques comme outil pour faciliter le processus d'évaluation et, surtout, pour rendre le document plus lisible par le responsable du traitement.* » - DPO externe italien.

> « *Presque systématiquement, j'illustre mes AIPD d'une matrice des risques. Il s'agit avant tout d'un outil de communication interne qui aide à rendre le document accessible et exploitable pour les décideurs qui, dans la plupart, ne sont pas des spécialistes de la protection de la vie privée. D'après mon expérience, une AIPD qui n'en comprend pas est trop facilement mise de côté sans être lue … Cela dit, je veille à présenter la matrice non pas comme un livrable autonome, mais comme la synthèse visuelle d'un processus analytique raisonné. Le responsable du traitement des données doit toujours être en mesure de répondre à la question suivante : « Pourquoi ce risque est-il positionné ici et pas ailleurs ? ».* » - DPO italien.

Si oui, quelles sont les caractéristiques de cette matrice ?

> « *La méthode d'évaluation des risques que j'utilise actuellement est encore en cours d'élaboration et fait l'objet d'améliorations progressives. Il s'agit d'un outil très complexe qui n'est pas facile à mettre en œuvre dans les PME, car il nécessite une expertise spécialisée qui, dans la plupart des cas, fait malheureusement encore défaut. Au sein d'une matrice 5x5, j'utilise un code couleur simple, facilement compréhensible même pour les utilisateurs non techniciens : vert (faible), jaune (moyen), orange (moyen/élevé), rouge (élevé/critique). Les seuils sont généralement les suivants, obtenus par multiplication de la vraisemblance et de la gravité : 1-4 vert ; 5-9 jaune ; 10-14 orange ; 15-25 rouge. En ce qui concerne la couleur verte, je reconnais effectivement qu'elle peut déclencher une réaction psychologique typique du type « tout va bien », conduisant parfois le responsable du traitement des données à considérer*

que le risque est totalement résolu. C'est un aspect sur lequel je vais me pencher, car même les éléments graphiques peuvent influencer la perception du risque. » - DPO italien.

« *Nous utilisons une matrice 4x4, avec trois couleurs (vert, jaune et rouge), mais avec une répartition différente de celle observée en France : nous ne colorons que trois cases en rouge et, symétriquement, que trois cases en vert, cela sans doute afin d'éviter que des cases vertes et rouges se touchent. Et, effectivement, cette allocation met au même niveau les risques V4/G1 et V1/G4 et leur affecte la même couleur… ce qui est étrange à la réflexion.* » - DPO allemand.

« *Ma norme actuelle est une matrice 4×4, en utilisant l'échelle ordinale à quatre niveaux dérivée de la méthodologie de la CNIL, qui reste la principale référence pour les DPO italiens en l'absence d'un outil émanant de notre autorité de contrôle. J'utilise généralement trois couleurs : vert, jaune/orange et rouge. Les directives du Garante n'imposent aucune palette spécifique, ce qui laisse une certaine liberté aux praticiens. J'ajoute une limite d'acceptabilité, que je considère comme essentielle : sans elle, la matrice ne peut répondre à la question décisive de savoir si une consultation préalable de l'autorité au titre de l'article 36 du RGPD est nécessaire. Pour les étiquettes sémantiques, je me suis éloigné du vocabulaire symétrique de la CNIL, où les mêmes termes sont utilisés pour les deux axes. Je trouve cela conceptuellement imprécis.* » - DPO italien.

« *J'ai l'habitude d'utiliser une matrice comportant quatre lignes et quatre colonnes ainsi que quatre couleurs : rouge, orange, jaune et vert.* » - DPO espagnol.

Ces caractéristiques ont-elles été définies de manière indépendante ou découlent-elles d'un outil ou d'une méthodologie spécifique ?

« *Les caractéristiques de la matrice ont été définies de manière autonome, bien qu'elles s'inspirent de plusieurs sources méthodologiques : l'outil PIA de la CNIL, la norme ISO/IEC 29134 et la méthodologie d'évaluation de la gravité des violations de données de l'ENISA. En Italie, aucun outil n'a atteint le niveau de pénétration du marché dont bénéficie l'outil PIA de la CNIL en France. Plusieurs outils proposés aux DPO italiens intègrent une matrice des risques, mais rares sont ceux (voire aucun) qui permettent une personnalisation significative de la sémantique, du choix et de la disposition des couleurs ou des limites d'acceptabilité.* » - DPO italien.

« *En Bavière, nous utilisons la plupart du temps l'illustration suggérée par notre autorité.* » - DPO allemand.

« *Je suis obligé d'utiliser la matrice qui m'est imposé par l'outil choisi par mon prédécesseur, même si quelque fois je sens bien qu'elle n'est pas adaptée.* » - DPO espagnol.

Dans votre pays, existe-t-il une pratique « standard » ou bien différentes approches ?

« *D'après mon expérience, il n'existe pas de pratique « standard » concernant la matrice des risques. Cependant, on observe une certaine convergence sur certains éléments : matrices 3x3 ou 5x5, distinction entre risque brut et risque résiduel, et utilisation de la couleur pour faciliter la lisibilité.* » - DPO italien.

« *En Italie, il n'existe pas de pratique « standard » pour les matrices de risques dans les AIPD, car le Garante n'a pas publié de méthodologie ou d'outil d'AIPD comparable au logiciel PIA de la CNIL. Un constat, cependant : de nombreux DPD opèrent en tant que consultants externes au service de plusieurs clients, et ceci dans différents secteurs. Cela crée une sorte de "normalisation", parfois au détriment de la profondeur analytique qu'exige une AIPD rigoureuse.* » - DPO italien.

« *Même si l'Autorité espagnole a publié un guide qui donne des exemples que l'on peut suivre - mais qui ne sont pas obligatoires - tous les DPO en Espagne ne font pas la même chose et il y a des différences, aussi bien en termes de structure des matrices que des couleurs utilisées.* » - DPO espagnol.

« *En Italie, il n'existe actuellement aucune pratique standardisée et universellement reconnue. L'autorité chargée de la protection des données n'a pas publié de lignes directrices spécifiques sur la structure de la matrice des risques dans les AIPD, se limitant à intégrer et à se référer aux lignes directrices du WP29/EDPB. En conséquence, différentes approches sont observées : dans certains cas, des matrices simplifiées (3x3) sont préférées ; dans d'autres, des grilles plus complexes sont adoptées ; certains praticiens s'inspirent des méthodologies de gestion des risques empruntées au domaine de la sécurité informatique (par exemple, les approches de l'ENISA), tandis que d'autres développent des cadres propriétaires. La terminologie et la définition des niveaux de risque font également l'objet de variations importantes.* » - DPO italien.

Ce sujet fait-il l'objet de discussions ou de débats au sein de votre communauté de DPO ?

« *J'ai l'impression que la matrice est encore traitée de manière quelque peu superficielle, davantage comme un « document à joindre » que comme un outil permettant d'améliorer réellement les décisions du responsable du traitement. Dans les PME, ce risque est amplifié car la priorité du client est souvent « de remplir le document », alors que l'objectif correct devrait être de faire de l'AIPD un outil de réelle gouvernance. Dans de trop nombreux cas, malheureusement, non seulement la matrice, mais aussi l'AIPD elle-même sont abordées avec une profondeur limitée, étant davantage perçues comme un document à produire que comme un outil d'analyse réelle du traitement.* » - DPO italien.

« *Les caractéristiques de la matrice des risques en tant qu'outil ne fait que très modestement l'objet de débats au sein de la communauté italienne des DPO. La discussion tend à se concentrer sur des questions de procédure (quand une AIPD est-elle nécessaire ? Que doit-elle contenir ?). Un débat qui prend de l'ampleur ici concerne la relation entre les AIPD réalisées au titre de l'article 35 du RGPD et les évaluations d'impact sur les droits fondamentaux formalisées au titre de l'article 27 du règlement sur l'IA : quels impacts sur l'avenir des méthodologies actuellement utilisées. Les praticiens italiens du droit de l'IA et les professionnels de la protection de la vie privée commencent à engager un dialogue interdisciplinaire pour tenter de trouver des réponses.* » - DPO italien.

« *Ce sujet n'a pas encore reçu le niveau d'attention qu'il mérite au sein de la communauté italienne des DPO. Il manque encore une discussion structurée qui pourrait conduire à l'identification de bonnes pratiques communes. Je pense qu'une plus grande standardisation – ou du moins la définition de critères minimaux communs – serait souhaitable afin de garantir une meilleure qualité et "comparabilité" des AIPD, même si l'analyse qualitative reste une composante essentielle de l'analyse et doit nécessairement être adaptée au contexte.* » - DPO italien.

En conclusion (temporaire)

J'aime à dire que l'AIPD aide le responsable de traitement (et toutes les parties prenantes) à s'inquiéter de manière intelligente, et que les matrices de risques qui illustrent nos AIPD sont des outils précieux pour aider nos responsables de traitement à prendre des décisions éclairées. Pour paraphraser Mark Twain, il ne faudrait pas qu'au contraire, elles les poussent à sous-estimer des risques qu'ils ont décidé de faire peser sur des tiers (« *Il y a trois sortes de mensonges : les mensonges, les sacrés mensonges et les ~~statistiques~~ matrices de risques* »).

Ne détenant pas la vérité, j'espère que le présent document suscitera réflexions et débats, notamment au sein de l'AFCDP, association française qui regroupe et représente les Délégués à la Protection des Données et, plus largement, tout professionnel intéressé ou concerné par la conformité au RGPD et à la loi

Informatique et Libertés, et je suis impatient de recueillir vos réactions, suggestions et propositions pour aboutir sur une représentation des risques pour les personnes qui soit « idéale ».

Un regard vers le futur

Plusieurs propositions formulées dans le Digital Omnibus auraient un effet important sur le sujet que je viens de développer si elles étaient adoptées. La moindre d'entre elles est la publication d'une liste unique, au niveau européen, des catégories de traitement qui exigent la réalisation d'une analyse d'impact. J'avoue avoir été surpris que les autorités n'aient pas pris l'initiative de s'entendre, notamment au sein du CEPD, pour y parvenir du premier coup. Mais les différences qui existent actuellement entre les listes nationales me semblent mineures. À titre d'exemple, Datatilsynet (autorité du Danemark) exige que « *Les opérations de traitement pour lesquelles une violation des données personnelles pourrait avoir un effet direct sur la santé physique ou la sécurité d'une personne physique* » fassent l'objet d'une analyse d'impact. On peut établir une correspondance avec la catégorie « *Traitements de données de santé mis en œuvre par les établissements de santé ou les établissements médico-sociaux pour la prise en charge des personnes* » qui figure dans la délibération n° 2018-327 du 11 octobre 2018 de la CNIL. Notons que la liste danoise ne comporte que huit catégories, là où la liste de la CNIL en comporte quatorze.

Il est une autre proposition qui m'inquiète davantage. Le CEPD serait chargé de proposer un modèle commun et une méthodologie harmonisée au niveau européen pour la réalisation des analyses d'impact. La formulation de l'Omnibus ne permet pas de savoir si cette méthodologie sera seulement proposée ou imposée. Le RGPD décrit actuellement à quoi on doit arriver en produisant une AIPD (et les lignes directrices du G29 liste des critères à respecter), mais n'impose en rien une méthode pour y parvenir. J'espère donc qu'il ne s'agira que d'une suggestion, qui sera sûrement d'une grande aide pour les DPO débutants, mais qui laissera les plus expérimentés continuer à exercer leur indépendance, y compris dans le choix de leur approche. Si, au contraire, il s'agit d'une obligation[73], plusieurs questions s'imposeront, dont celles-ci : faudra-t-il « reprendre » les AIPD déjà réalisées pour les porter au nouveau standard ? En combien de temps les éditeurs d'outils seront ils en mesure de s'adapter… et à quels coûts pour leurs clients ? L'outil PIA de la CNIL sera-t-il retiré ou modifié en profondeur ?

Je redoute également que la méthodologie unique soit à nouveau une resucée de l'une des méthodes d'analyse de risque tant bien que mal (et plutôt mal) adaptée à l'analyse d'impact. Je ne reprends pas ici les éléments que j'ai évoqués *supra*, mais j'ai crainte de voir s'imposer une méthode focalisée sur la cybersécurité et les DPO contraints à se voir imposer des approches qui aboutissent à de piètres résultats. Le moindre mal serait de voir sélectionnée la méthode EBIOS Risk Manager[74] (Expression des Besoins et Identification des Objectifs de Sécurité), qui est ainsi présentée par l'ENISA : « *EBIOS Risk Manager est une méthode de gestion des risques liés à la sécurité de l'information, créée sous l'égide du Secrétariat général de la défense et de la sécurité nationale (France), conforme aux normes ISO 31000 et ISO/IEC 27005, et permettant de répondre aux exigences de gestion des risques de la norme ISO/IEC 27001.* ».

Profitera-t-on des travaux qui vont être menés par le CEPD pour étudier les parties qui pourraient être mutualisées en cas de formalisation combinée d'une analyse d'impact sur la protection des données au titre

[73] Dans son document *Risk Management Standards - Analysis of standardisation requirements in support of cybersecurity Policy*, publié en 2022, l'ENISA formule le souhait suivant : « Les décideurs politiques de l'UE devraient rendre obligatoires certaines méthodologies ou certains outils d'évaluation des risques pour des secteurs spécifiques, lorsque cela s'avère nécessaire. ».

[74] Dans son analyse du Digital Omnibus de janvier 2026, NYOB se montre favorable à cette possible évolution : « *Dans l'ensemble, NYOB suggère d'adopter cette disposition telle qu'elle est proposée. Cette suggestion s'éloignerait de l'idée d'une approche dite « fondée sur les risques », avec d'innombrables facteurs vagues, où le responsable du traitement est largement laissé libre de décider si un article du RGPD s'applique ou non à lui. Cette approche permet au contraire une application plus objective et plus simple de la loi, ce qui améliore la sécurité juridique de toutes les parties prenantes.* ». J'avoue ne pas savoir sur quoi s'appuie cet optimisme béat, puisqu'à ce stade nous ne savons rien de la future méthodologie qui sortira des travaux du CEPD... fort probablement à nouveau une approche fondée sur les risques, avec d'innombrables facteurs vagues et où le responsable du traitement a de toute façon le dernier mot.

de l'article 35 du RGPD et d'une analyse d'impact sur les droits fondamentaux[75] (ou FRIA pour *Fundamental Rights Impact Assessments*) au titre de l'article 27 du règlement européen sur l'intelligence artificielle ? Je l'espère.

Le Digital Omnibus propose également d'exclure de la définition des données Art.9 celles qui y figurent actuellement de façon indirecte. Ce serait un recul par rapport à l'arrêt CJUE du 1er août 2022 (affaire C-184/20) qui demandait à ce que soit considéré comme un traitement de données sensibles un traitement portant non seulement sur des données intrinsèquement sensibles, mais également sur des données dévoilant indirectement, au terme d'une opération intellectuelle de déduction ou de recoupement, des informations de cette nature. Si cette modification est adoptée, il faudra veiller à n'en tenir aucun compte lors de la réalisation d'AIPD, au risque de passer à côté d'éléphants dans le couloir, comme c'est déjà le cas aujourd'hui avec certains outils qui, pour vous faciliter la vie, se contentent de soulever une dizaine de questions avant de vous délivrer une analyse d'impact « clé en mains ». Parmi ces questions en figure une sur la présence (ou pas) dans le projet de traitement de données dites « sensibles » (c'est-à-dire relevant de l'article 9.1 du RGPD). Si l'on ne force pas à penser qu'une donnée anodine peut se transformer en information sensible dans certains contextes, le résultat pourra être catastrophique. Tout DPO expérimenté sait que le caractère *sensible* d'une donnée personnelle n'est pas seulement déterminé par sa nature mais peut l'être aussi par un contexte. Ainsi, les adresses figurent rarement sur les listes de données sensibles, et pourtant leur divulgation peuvent être très dangereuses si elles sont divulguées. Aux USA, l'actrice Rebecca Shaeffer a été assassinée lorsqu'un harceleur a obtenu son adresse auprès du *Department of Motor Vehicles* (qui gère les permis de conduire). Ce drame a entraîné l'adoption d'une la loi fédérale sur la protection de la vie privée des conducteurs, le *Driver's Privacy Protection Act*.

Autre projet qui pourrait éventuellement avoir des conséquences sur la réalisation d'AIPD et sur leur qualité : pour rationaliser les modalités de notification des différents « incidents » que les organismes doivent notifier auprès de différentes autorités afin de respecter plusieurs textes (dont les violations de données personnelles qui doivent être notifiées auprès de la CNIL au titre du RGPD), un guichet unique européen devrait être créé pour accueillir les signalements au titre de la directive NIS 2, du règlement DORA, du RGPD, du règlement eIDAS et de la directive sur la résilience des entités critiques[76] (CER). Ce point d'entrée devrait être supervisé par l'ENISA. Dès lors, la disparité observée actuellement au niveau européen entre les informations qui doivent être délivrées actuellement par un responsable de traitement en cas de violation de données personnelles devrait disparaitre. Mais il est possible que la nouvelle notification s'aligne vers le haut… et qu'il soit demandé de fournir l'AIPD qui a été (aurait dû être) réalisée sur le traitement qui a fait l'objet de la violation. Une bonne façon d'obtenir que les analyses d'impact soient réalisées et qu'elles soient menées avec l'objectif réel de réduire les risques que l'on fait courir aux personnes concernées.

Enfin, le Digital Omnibus renvoie au Comité Européen de Protection des Données (CEPD) pour formaliser une liste des circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'entraîner un risque élevé pour les droits et libertés d'une personne. Gageons que ce livrable influera en profondeur sur l'évaluation du niveau de risque dans le cadre d'une AIPD.

Il reste donc à espérer que le CEPD entendra les DPO européens sur tous ces sujets.

[75] Cf. *Analyses d'impact sur les droits fondamentaux : Qu'est-ce que c'est ? Comment fonctionnent-elles ?*, CEPDO, Janvier 2025

[76] Mais pas au titre du Règlement sur l'Intelligence Artificielle.

Dédicace et remerciements

Je dédie ce travail à tous les DPO qui tentent d'exercer leur métier avec persévérance, compétence, intégrité et indépendance.

La rédaction de ce document m'a donné l'occasion d'échanger avec de nombreuses consœurs et confrères DPO, y compris à l'étranger. Merci à Pablo Garrote Crespo (DPO de Grupo Igualatorio Médico Quirúrgico), Charlaine Berendt (Group Data Protection Officer, Aenova, Munich), Henry Simwinga (Data Protection Manager, Forest Stewardship Council, Cologne), Nadia Arnaboldi (Vice-Présidente de CEDPO), Massimiliano Pappalardo (Asso DPO), Andrea Repetto (Asso DPO) et Filippo Bianchini (Asso DPO). Un grand merci également à Erik Boucher de Crevecoeur (CNIL), Patrick Blum (ancien Délégué général de l'AFCDP), Jérôme de Mercey (co-fondateur de Dastra), Yann-Hervé Beulze (ancien RCCI, RSSI, DPO et Correspondant risques de Groupama Asset Management), Christophe Champoussin (Anaxia Conseil, Administrateur AFCDP), Edouard Schlumberger (co-fondateur de Leto), Alessandro Fiorentino (Adequacy), Mehdi Sbai-Idrissi et Benjamin Baratta (Witik) et Edouard Schlumberger (Co-fondateur de Leto).

L'auteur

Bruno Rasle se définit comme un « monomaniaque » de la conformité au RGPD et pratique cet art martial sous trois formes : à titre professionnel, il a été délégué à la protection des données mutualisé pour l'une des branches de la Sécurité sociale, désigné pour plus d'une centaine de responsables de traitement ; à titre bénévole, il est l'un des tous premiers membres de l'AFCDP et a été son délégué général pendant une douzaine d'années ; en tant qu'enseignant enfin, en tant que chargé de cours au sein de la formation la plus ancienne et du niveau le plus élevé en Europe (il forme les professionnels de la *Privacy* depuis 2007). Il a également pris une part active dans la création du métier de Correspondant Informatique et Libertés (puis de Délégué à la Protection des Données). Il est coauteur des ouvrages suivants : *Halte au Spam* (Eyrolles, 2003) ; *Correspondant Informatique et Libertés : bien plus qu'un* métier (AFCDP, 2015) ; *Droit à l'oubli* (Larcier, 2015) ; *Se préparer au RGPD* (Éditions législatives, 2017). Il a créé l'Université AFCDP des DPO (et a été son organisateur jusqu'en 2020), l'Index AFCDP du droit d'accès et le *Job board* des DPO (AFCDP). Bruno Rasle est le co-auteur du code de déontologie du DPO et de la version annotée, commentée et indexée du RGPD mise à disposition par l'association. Il a participé à la création de CEDPO (Confédération européenne des associations de professionnels de la protection de la vie privée) dont il a été *Board Member*.

Ses publications sont nombreuses (« *Le DPO : source d'inconfort ou créateur de valeur ?* », « *Communication aux victimes d'une violation de données : aller plus loin que le RGPD ?* », « *Il faut sauver le soldat DPO !* », « *La sécurité des données personnelles enfin prise au sérieux ?* », « *Rapport CEPD sur le droit d'accès RGPD : Tout ça pour ça ?* », « *Demandes de droits RGPD : pas de formulaire apparaissant comme obligatoire* » , « *RGPD : Ils ont inventé la mitrailleuse à demandes de droit d'accès* », « *Le registre RGPD n'est pas une fin en soi* », « *RGPD : Cette autorité de contrôle impose-t-elle des exigences irréalistes ?* », « *20 ans de l'AFCDP : souvenirs, souvenirs ...* », « *Faut-il être parano pour faire un bon PIA ?* », « *La purge des données – Un effort qui en vaut la peine* », « *Pour une désignation idéale du DPO* », « *Courteline rend le sourire aux DPO* », « *Collègues DPO : le bilan annuel est un outil précieux : faisons-en une bonne pratique* », « *PSSI : contrainte ou opportunité ?* »), de même que ses interventions en conférence (« *Cookie et Widget : peut-on vraiment surfer tranquille ?* », Université AFCDP 2011, « *Synergie entre RSSI et CIL* » , Cesin 2012 ; « *Mise en conformité des Zones de Libre Commentaire* », Université AFCDP 2013 ; « *Privacy by Design : le rôle clé des développeurs* », AtoutFox 2013 ; « *CPO & CSO : Bridging the gap* », IAPP Bruxelles 2013 ; « *Les méthodes agiles sont-elles Privacy-compatibles ?* », Cloud Week Paris 2015 « *La Blockchain est-elle soluble dans le RGPD ?* », AG AFCDP 2017 ; « *Le RGPD, évolution ou révolution ?* », Journées JCAS 2017 ; « *Que sommes-nous ? Responsable de traitement ? Responsable conjoint ? Sous-traitant ?* », AG AFCDP 2019 ; « *Comment auditer sa gestion des droits d'accès ?* », Université AFCDP 2021 ; « *Créer et animer un réseau de RIL* », Université AFCDP 2022 ; « *Communication d'une violation de données aux victimes : aller plus loin que le RGPD ?* », Université AFCDP 2025).

Outre son enseignement au sein du Mastère Spécialisé « *Management et Protection des Données Personnelles* » de l'ISEP, du Mastère DPO d'Oteria et du DU DPO de Panthéon-Assas, il propose des formations courtes pour le compte d'Anaxia Conseil[77] (« *L'informatique appliquée au RGPD* », « *Réaliser une Analyse d'Impact – De la théorie à la pratique* », « *Violations de données : pour ne pas subir* », « *Contrôle de la CNIL – S'y préparer, le gérer, y survivre* », « *Être un DPO efficace dès les premiers jours* », « *Pour une gestion efficace des droits RGPD* »).

[77] *www.anaxia-conseil.fr*